UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO

LA PROTECCIÓN DE DATOS PERSONALES : ESTUDIO COMPARATIVO EUROPA-AMÉRICA CON ESPECIAL ANÁLISIS DE LA SITUACIÓN ARGENTINA

MEMORIA PARA OPTAR AL GRADO DE DOCTOR
PRESENTADA POR

Carlos Eduardo Saltor

Bajo la dirección del doctor

Emilio Suñé Llinás

MADRID, 2013

UNIVERSIDAD COMPLUTENSE DE MADRID
Facultad de Derecho

La Protección de Datos Personales:

Estudio Comparativo Europa-América con especial análisis de la situación Argentina

TESIS DOCTORAL PRESENTADA POR

CARLOS EDUARDO SALTOR

DIRECTOR:

PROF. DR. D. EMILIO SUÑÉ LLINÁS

MADRID, 2013

ÍNDICE

PÁG.

ABREVIATURAS 7

RESUMEN EN INGLÉS 11

Introduction 11

Objective: Research Content 12

Conclusions / Results 14

Bibliography 15

CAPÍTULO I: JUSTIFICACIÓN 17

1.- Cuestiones metodológicas 17

1.1.- Hipótesis 20

1.2.- Punto de partida 20

1.3.- Antecedentes 22

2.- Intimidad y procesamiento de datos 23

2.1.- Sobre el concepto de derecho a la intimidad 28

2.2.- Diferencias con otras manifestaciones de la personalidad 39

2.2.1.- Lo confidencial 39

2.2.2.- Lo secreto 40

2.2.3.- Lo íntimo 40

2.2.4.- Honor y propia imagen 44

2.2.5.- Usos sociales y conducta del sujeto 48

2.2.6.- Derecho al olvido 51

2.3.- Intimidad y autodeterminación informativa 56

2.4.- Intimidad y protección de los datos 65

2.5.- Evolución histórica de la idea de intimidad 73

2.5.1.- Edad antigua 74

2.5.2.- Edad Media 78

2.5.3.- Edad Moderna 82

2.5.4.- Edad Contemporánea 85

2.5.5.- Siglos XX y XXI 87

2.6.- La intimidad de las personas jurídicas 96

3.- Reconocimiento Internacional 98
3.1.- Recomendación de la OCDE 107
4.- Técnicas legislativas aplicadas a la protección de datos 109
4.1.- Leyes Sectoriales 109
4.2.- Leyes Ómnibus 110
5.- Habeas Data 111
6.- Jurisprudencia del Tribunal Constitucional español sobre protección de datos 114
6.1.- Sentencia 290/2000 de 30 de noviembre 115
6.2.- Sentencia 254/1993 de 20 de julio 116
6.3.- Sentencia 292 de 30 de noviembre de 2000 123
6.3.1.- Importancia de la STC 292/2000 127
6.3.2.- ¿Protección de datos o autodeterminación informativa en la STC 292/2000? 132
7.- Principios de la protección de los datos de carácter personal 135
8.- Autoridad de control para la protección de datos 140
8.1.- Autoridad de control independiente 142
8.2.- Autoridad de control dependiente del Poder Ejecutivo 146
8.3.- Sistema de control judicial de aplicación de la ley 148
8.4.-El encargado de protección de datos 149
9.- Datos personales y telecomunicaciones 150
CAPÍTULO II: PROTECCIÓN DE DATOS EN ESPAÑA Y EUROPA 155
1.- El Consejo de Europa 155
1.1.- Las Resoluciones (73) 22 y (74) 29 del Comité de Ministros 155
1.2.- El Convenio 108 del Consejo de Europa 156
2.- Antecedentes en el derecho europeo 163
2.1.- Acuerdo de Schengen de 14 de junio de 1985 166
2.2.- Directiva 95/46/CE 169
2.3.- Directiva 58/2002/CE del Parlamento Europeo y del Consejo 174
2.4.- Directiva 97/66/ CE 177

2.5.- Nuevas normas europeas 179
2.6.- Proyecto de la Comisión Europea del año 2012 180
2.6.1.- Control ciudadano 183
2.6.2.- Protección de datos en el mercado digital 184
2.6.3.- Globalización y protección de los datos 186
2.7.- La protección de datos en la Constitución Europea 187
3.- España 190
4.- Alemania 201
5.- Austria 209
6.- Bélgica 215
7.- Dinamarca 222
8.- Francia 226
9.- Grecia 237
10.- Holanda 243
11.- Irlanda 246
12.- Italia 250
13.- Portugal 252
14.- Reino Unido 256
15.- Suecia 263
16.- Noruega 268
CAPÍTULO III: PROTECCIÓN DE DATOS EN AMÉRICA 272
1.- Estados Unidos de América 274
1.1.- Autoridad de aplicación en EEUU 281
1.2.- Bancos de Datos de Información de Crédito 281
1.3.- Seguridad 284
2.- Bolivia 284
3.- Brasil 287
4.- Perú 294
5.- Nicaragua 301
6.- Panamá 304

7.- Canadá 309
8.- Colombia 313
9.- Chile 320
10.- Costa Rica 324
11.- Ecuador 333
12.- México 339
13.- Paraguay 345
14.- Uruguay 347
15.- Venezuela 354
16.- El Salvador 358
17.- MERCOSUR 360
18.- Cuadro comparativo de algunas normas americanas 365
CAPÍTULO IV: PROTECCIÓN DE DATOS EN ARGENTINA 366
1.- Un nuevo derecho en Argentina 366
2.- Intimidad y datos personales en la historia argentina 367
3.- Reforma constitucional de 1994 375
3.1.- Doctrina y jurisprudencia 377
3.2.- *Habeas Data*: naturaleza jurídica y trámite procesal 378
3.2.1.- Legitimación activa en la acción de *habeas data* 381
3.2.2.- Legitimación pasiva en la acción de *habeas data* 384
4.- Desarrollo normativo del artículo 43 ter. 384
4.1.- La vetada ley sobre *habeas data* N° 24.745 384
4.2.- Decreto Nacional 1616/96 385
4.3.- Proceso de formación de la Ley 25.326 392
4.4.- Decreto Nacional 1558/2001 393
5.- Ley 25.326 de Protección de Datos Personales 396
5.1.- Objeto de la ley 25.326 400
5.2.- Datos personales y otros conceptos 401
5.3.- Principios de protección de datos 403
5.3.1.- Licitud de la formación de archivos de datos 403

5.3.2.- Prohibición de acumulación de datos sensibles 403
5.3.3.- Prohibición de bancos de datos que no reúnan condiciones de seguridad 404
5.3.4.- Principio de confidencialidad 404
5.3.5.- Principio de Buena Fe 406
5.4.- Cesión de Datos Personales 407
5.5.- Obligaciones del cesionario 407
5.6.- Transferencia internacional de datos 409
5.7.- Derechos de los titulares de los datos 410
5.7.1.- Derecho a la información 410
5.7.2.- Derecho de acceso 411
5.7.3.- Derecho a conocer el contenido de la información 411
5.7.4.- Derecho de rectificación de datos personales 412
5.7.5.- Derecho de actualización de los datos personales 412
5.7.6.- Derecho de supresión de los datos personales 413
5.7.7.- Derecho a impugnar valoraciones personales 413
5.7.8.- Gratuidad en el ejercicio de los derechos del titular 413
5.7.9.- Excepciones 413
6.- Comisiones legislativas 414
7.- Usuarios y responsables de archivos, registros y bancos de datos 415
8.- Archivos, registros o bancos de datos privados 417
9.- Prestación de servicios de información crediticia 418
10.- Archivos, registros o bancos de datos con fines de publicidad 420
11.- Archivos, registros o bancos de datos relativos a encuestas 420
12.- Órgano de control 420
13.- Códigos de conducta 423
14.- Sanciones administrativas y penales 425
15.- Etapas del proceso de protección de datos personales 427
15.1.- Etapa extrajudicial 427
15.2.- Etapa judicial de protección de datos personales 428

16.- Jurisprudencia 437
16.1.- Jurisprudencia anterior a la reforma constitucional de 1994 437
16.2.- Jurisprudencia posterior a la reforma constitucional de 1994 438
17.- Antecedentes en el derecho público provincial argentino 443
17.1.- Protección de datos en la Provincia de Tucumán (Argentina) 456
CAPÍTULO V: CONCLUSIONES 465
1.- Problema 465
1.1.- Tecnología y procesamiento de datos 465
1.2.- Uso masivo de las TIC 466
1.3.- Efectos de la conducta de las personas en el mundo virtual 467
1.4.- Las Redes Sociales 469
2.- Recolección de Datos 470
2.1.- Utilidad del método comparativo 470
2.2.- Legislación de protección de datos personales 471
2.3.- La jurisprudencia 473
2.4.- Legislación Europea 474
2.5.- Legislación americana 474
2.6.- La protección de datos personales en Argentina 476
3.- Resultados 480
Primera conclusión 480
Segunda conclusión 480
Tercera conclusión: propuestas para mejorar la legislación Argentina 483
Reflexión final 485
RECURSOS BIBLIOGRÁFICOS 487
BIBLIOGRAFÍA 487
WEBGRAFÍA 494
LEGISLACIÓN CONSULTADA 502
INFORMACIÓN ADMINISTRATIVA 508
ÍNDICE DE CAPÍTULOS 509

ABREVIATURAS

AATC	Autos del Tribunal Constitucional
ACPD	Agencia Catalana de Protección de Datos
AEPD	Agencia Española de Protección de Datos Personales (España)
APDCM	Agencia de Protección de Datos de la Comunidad de Madrid (España)
APDPV	Agencia de Protección de Datos del País Vasco
AS	Acuerdo de Schengen
ATC	Auto del Tribunal Constitucional
BGDS	Ley Federal de Protección de Datos Personales (Alemania)
BJC	Boletín de Jurisprudencia Constitucional (España)
BJE	Boletín de Jurisprudencia Extranjera (Editado en España)
BVK	Unión Profesional de Crédito (*Beroepsvereniging van hetKrediet,* Bélgica)
C. de E.	Consejo de Europa
CA	Constitución Argentina
CB	Constitución de Bolivia
CBRA	Constitución de Brasil
CCA	Código Civil (Argentina)
CCE	Código Civil (España)
CCH	Constitución de Chile
CE	Constitución Española de 1978
CE	Constitución de Europa
CEC	Centro de Estudios Constitucionales
CEDH	Convenio Europeo de Derechos Humanos
CEDH	Convenio Europeo de Derechos Humanos
CEPC	Centro de Estudios Políticos y Constitucionales
CES	Constitución Española de 1978
CGPJ	Consejo General del Poder Judicial
CIDH	Corte Interamericana de Derechos Humanos
CIS	Centro de Investigaciones Sociológicas
CM	Constitución de México
CNA	Constitución Nacional (Argentina)
CNIL	Comisión Nacional de Informática y Libertades (Francia)
CNIL	Comisión Nacional para la Informática y las Libertades de Francia.
CPE	Código Penal (España)
CPA	Código Penal (Argentina)
CPAR	Constitución de Paraguay
CPCT	Código Procesal Constitucional de la Provincia de Tucumán (Argentina)
CPE	Constitución de Perú
CPER	Constitución de Perú
CSJNA	Corte Suprema de Justicia de la Nación (Argentina)
CSJT	Corte Suprema de Justicia de la Provincia de Tucumán (Argentina)

CU	Constitución de Uruguay
DNPDP	Dirección Nacional de Datos Personales (Argentina)
f.j.	Fundamento Jurídico
fci.	Fuente consultada en Internet
IFAI	Instituto Federal de Acceso a la Información y Protección de datos (Méjico)
LDDP	Ley de Derechos y Deberes de los Pacientes
LEC	Ley de Enjuiciamiento Civil
LECr	Ley de Enjuiciamiento Criminal
Ley 25326	Ley Nacional de Protección de Datos Personales (Argentina)
LGSE	Ley General de Sanidad (España)
LGT	Ley General Tributaria
LMF	Ley de Medidas Fiscales
LO	Ley Orgánica
LOPD	Ley Orgánica de Protección de Datos (España)
LOPJ	Ley Orgánica del Poder Judicial
LOTC	Ley Orgánica del Tribunal Constitucional
LOREG	Ley Orgánica de Régimen Electoral General
LORTAD	Ley Orgánica de tratamiento automatizado de datos de carácter personal de 1992
LOVI	Ley Orgánica de Video Vigilancia
LPDFR	Ley de Protección de Datos de Francia Nº 78-77
LPDMX	Ley de Protección de Datos de México
LPDVPCH	Ley de Protección de la Vida Privada (Chile): Ley Nº 19628
LRJAP	Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común
LTRA	Ley sobre Técnicas de Reproducción Asistida
RCCH	Registro Civil (Chile)
RDP UNED	Revista de Derecho Político de la Universidad Nacional de Educación a Distancia
RGIT	Reglamento General de Inspección de Tributos
RGLJ	Revista General de Legislación y Jurisprudencia
SIS	Sistema de Información de Schengen
SJCCCT	Sentencia de Juzgado Civil y Comercial Común de Tucumán (Argentina)
SSTC	Sentencias del Tribunal Constitucional
SSTEDH	Sentencias del Tribunal Europeo de Derechos Humanos
STC	Sentencia del Tribunal Constitucional
STCA	Sentencia del Tribunal Constitucional (Alemania)
STCE	Sentencia del Tribunal Constitucional (España)
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TCA	Tribunal Constitucional de Alemania

TCE	Tribunal Constitucional de España
TEDH	Tribunal Europeo de Derechos Humanos
TIC	Tecnologías de la Información y de las Comunicaciones
TJUE	Tribunal de Justicia de la Unión Europea
TUE	Tratado de la Unión Europea
VV. AA.	Varios Autores

RESUMEN EN INGLÉS

PERSONAL DATA PROTECTION: A COMPARATIVE STUDY EUROPE AMERICA WITH SPECIAL SITUATION ANALYSIS ARGENTINA.

Introduction

The information technology and communications have proven to be suitable for the processing and treatment of large volumes of information, but the effects of computer and telematics treatment of personal data without control, adversely affecting people's privacy. For this reason, the technology penetration in the lives of people we facing a new ethical and legal problems as the unlimited power of the people can know about both the state and the private sector, accumulate and process personal data for in some cases, an abuse of illegal use and even a social control over human beings.

True, states, institutions and different organizations need contemporary world of modern information technologies and communication networks to acquire, assess and classify the information that allows them to make decisions aimed at the goals and objectives of the general welfare which they were created. But it is also true that these different interconnect technologies allow data files and get them information that traces a detailed profile of the people, which is a tool who has the power to use it, both in the public and private sectors.

The legal system must set limits on the accumulation and processing of personal data for their abuse not harm the privacy and informational self-determination of individuals of our species.

In this scenario the data protection is now central to all laws. Essential part of all constitutional rights, while having a direct impact on the citizen, not only on a national but also international. The so-called ICT (information and communication) are basic tools of social and economic development, as well as an area of adjustment needed to the right.

On the legal data protection has a volume of casuistry unfit for the knowledge areas of law, for the purpose of computing and telecommunications in this area. To this we must add a dizzying need for adaptation of legal science developments and technical possibilities offered by technological developments.

Becomes even more complex study of the protection of personal data necessary for the regional and international levels should be regulation, since communication networks do not respect State boundaries.

And we should add that the massive use that currently gives humanity to technology is also a new challenge to the law in general and to data protection in particular.

Objective: Research Content

Given this reality, the comparison of national regulations in Europe and America (with special analysis of the laws of Spain and Argentina) in an area as technical as the protection of personal data, presents numerous advantages. The comparative method, based on analogical hermeneutics allows us to see the weaknesses and the strengths of the legislation. Through this method display better the legal and clearly seen as a normative imperative it generates different factual situations.

The objective of this thesis is to compare the right to protection of personal data in Europe and America with special analysis of the laws of Spain and Argentina. For this, the study of the concept of privacy and its difference from other similar concepts, continues the historical evolution accompanying the birth of the new right to informational self-determination or protection of personal data.

Once focused on this new right to informational self-determination or protection of personal data this thesis studies achieved international recognition (OECD and Council of Europe), interpreted by jurisprudence on its scope,

operability, autonomy and legislative techniques applied in comparative law for its regulation.

In comparative law review some rules governing the right to protection of personal data in Europe (resolutions and directives of the European Union), Spain, Germany, Austria, Belgium, Denmark, France, Greece, Holland, Ireland, Italy, Portugal, UK, Sweden and Norway. In these countries (all EU members) homogenized law is observed by European directives. In all of them is common to find a right to protection of personal data that provides consolidated data protection principles, a clear claim process, enforcement bodies independent of the executive and explicit rules of international data transfer. The EU envisages a process of consolidation rules for greater homogeneity of the data protection legislation, embodied in the draft European Regulation on the Protection of Personal Data of 2012.

Studying the right to data protection in the Americas found a different reality. America started in the 1990s a process of incorporation of standards of protection of personal data is not yet complete. We found a state of evolution rules, still open, incorporation of constitutional in most states in the Americas. Constitutional provisions of the American constitutions have adopted for the protection of personal data including action under the different constitutions, is direct a constitutional guarantee that goes by the name of habeas data.

In some of these countries (not all) there are rules implementing the constitutional provisions of habeas data, but these laws are not uniform among them. In most cases you do not have an enforcement body and the few states that have created, not given autonomy or independence from the Executive.

Our study observed the laws of MERCOSUR, Argentina, United States, Bolivia, Brazil, Peru, Nicaragua, Panama, Canada, Colombia, Chile, Costa Rica, Ecuador, Mexico, Paraguay, Uruguay, Venezuela and El Salvador. In none of these laws the legislature has considered the existence of a body or control authority independent of the executive.

The importance of controlling authority regarding the protection of personal data is evaluated by observing the absence or weakness that results in excessive judicialization of procedures for habeas data. We note that when people do not have legal protection of personal data by government organized and supervised by an independent supervisory authority, has no choice but the necessary prosecution of their claims. Sometimes these lawsuits arise only to gain access to personal data concerning the owner of that information. Not so in states that have a strong control authority and independent, as the prosecution of the claim is an exception because most lawsuits are avoided by a clear complaints procedure, which form substance court before the watchdog.

The absence of a uniform law with global reach for the protection of personal data protection weakens a region or state can give people and hinders international cooperation and economic relations, business, labor, scientific requiring international transfer Data for operation.

Conclusions / Results

After studying comparative law, this thesis draws the following conclusions:

First Conclusion: To reduce the injury to the right to privacy and informational self-determination caused by the automated processing of personal data is necessary to develop specific legislation to protect personal data with global reach, to establish a process to access and correct course along the control of a law enforcement specialist, independent and autonomous of the executive branch of the state.

Second Conclusion: The regulation rules on personal data protection must be completed with a logical sequence of effectiveness: real and effective protection, which is achieved not only with legal recognition. It is also necessary:

a) The citizen awareness about the need to provide protection for your personal data.

b) The citizen awareness of the scope and possibilities of the right to protection of personal data.

c) Ensuring effective State and its operators the right to protection of personal data.

d) The constant adaptation laws protecting personal data.

Bibliography

* Alderman, E. C. Kennedy The Right to Privacy. Ed Random House, New York (USA), 1997.
* Basterra, M. I. Protection of Personal Data. Law 25,326 and Disc. 1558-1501 Annotated. Provincial Constitutional Law.Latin America and Mexico. Editorial Ediar – National Autonomous University of Mexico (UNAM). Buenos Aires / Mexico DF, 2008.
* Cattaruzza, A.; Galbiati, R.; Panieri, B., and Zampetti, A. Dei dati personali Guardianship. 2nd ed. Editorial. Buffetti Editori Multimedia. Buffetti Group. Rome 1998.
* Murillo de la Cueva, Lucas. The right to informational self-determination. Editorial Tecnos. Madrid, 1990.
* Murillo de la Cueva, Paul Lucas. Computing and Data Protection (Study of Law 5/1992, regulating the Automatic Processing of Personal Data). Notebooks and Debates No. 43. Center for Constitutional Studies. Madrid, 1993.
* Ortega y Gasset, J. Meditation technique. Editorial Revista de Occidente, Castilian 3rd edition, London, 1957.
* Palazzi, P. The Protection of Personal Data in Argentina. Errepar Ed. Buenos Aires, 2004.
* Luño Perez, A. Human rights, rule of law and constitution. Editorial Tecnos, 5th Edition. Madrid, 1995.

* Peyrano, G. Legal regime of personal data and habeas data. Editorial Lexis Nexis - Depalma.Buenos Aires, 2001.

* Puccinelli, O. Habeas Data in Indoiberoamérica. Temis Ed. Bogotá, 1999.

* Rebollo Delgado, L. Fundamental Rights and Data Protection. Editorial Dykinson. Madrid, 2004.

* Rebollo Delgado, L. The fundamental right to privacy. Editorial Dykinson (2nd edition). Madrid, 2005.

* Suñé Llinás, E. "The protection of privacy in the telecommunications sector." Notice published in the Proceedings of the twelfth meeting on IT and Law 98/99, (work coordinated by Miguel Angel Rodriguez Davara). Editorial Aranzadi. Pamplona, 1999.

* Suñé Llinás, E. Computer Law Treaty. Volume I: Introduction and Personal Data Protection. Second Edition (Updated by Cristina AlmuzaraAlmaida). Editorial Publication Services Law School of the Universidad Complutense de Madrid. Madrid, 2002.

* Suñé Llinás, E. Santamaría and Ramos, F. Commentary on Art. 43. Responsible and processors, p. 2017. Published in: Troncoso Reigada A. (Director). Commentary on the Law on Protection of Personal Data. Civitas and Thomson Reuters Editorial (Editorial Aranzadi). Pamplona (Spain), 2010.

* Warren, S.; Brandeis, L. "The Right to Privacy". Journal of Harvard University: Harvard Law 4. Rev. Cambridge, Massachusetts (USA), 1890.

* Urabayen, M. Private Life and Information. A permanent conflict. EUNSA (Publications of the University of Navarra SA). Zaragoza (Spain), 1977.

Capítulo I: JUSTIFICACIÓN

1.- Cuestiones metodológicas

El método que proponemos para desarrollar esta investigación es el estudio comparado de los textos de las constituciones, leyes o normas que traten el derecho a la protección de datos personales de Europa y América. Y dentro de estos dos continentes, nos focalizaremos en el contenido de las normas de España y Argentina, junto con la interpretación que ha dado la doctrina y la jurisprudencia a este tema.

Consideramos necesaria la observación comparativa para encontrar coincidencias y diferencias en materia de derecho a la protección de los datos personales. La Unión Europea legisló en la materia aprobando Directivas y normas específicas para uniformar la regulación de los datos personales en sus Estados miembros. Por este motivo enunciaremos sintéticamente la legislación que protege los datos personales de cada Estado miembro de la Unión Europea y nos detendremos en un estudio más profundo de la norma española, estructurada en base a la Directiva 95/46/CE (matriz europea), la doctrina y la jurisprudencia en la materia.

La relación entre los textos legales de España y de Argentina es directa, ya que la legislación española fue el modelo normativo, a partir del cual se sancionó la actual ley argentina sobre Protección de Datos Personales, que a su vez fue la primera norma de protección de datos personales en América. Por esta razón tendremos en cuenta especialmente la comparación entre la legislación española y argentina en la materia, sin perder de vista la diferente realidad en la que se aplica cada una de ellas.

El método elegido en esta tesises el método comparativo por las siguientes razones:

1. En la Metodología científica suelen distinguirse tres métodos generales: a) el deductivo o demostrativo o axiomático o hipotético-deductivo; si se aplican las reglas básicas del razonamiento (algoritmos) se llegan a conclusiones necesarias o altamente probables, como en las matemáticas, la lógica y las ciencias; b) el inductivo, que es un método que no sirve para la justificación científica, pero que es útil para la búsqueda de hipótesis; sus conclusiones siempre son inválidas (algunas veces verdaderas y otras falsas); c) el analógico que, dados dos estados de cosas, considera sus semejanzas y proporciones; sus conclusiones tampoco son válidas sino indeterminadas en cuanto a su verdad. Por supuesto, estos tres métodos tienen una complejidad epistemológica que no es posible abarcar en pocas páginas.

2. En el uso corriente, "analogía" significa también "comparación" entre dos o más estados de cosas, con el objeto de encontrar posibles semejanzas o características comunes. En la segunda mitad del siglo XIX se advirtió que este método es apto para los estudios historiográficos, y de allí que se lo utilizara en la Lingüística comparada, en la Historia comparada de las religiones o de las literaturas, etc. Pero también resultó útil, al menos en un comienzo, en algunas ciencias naturales como la geología, la geomorfología, la botánica, etc. Hay que recordar que, en ningún caso, las conclusiones analógicas o comparativas tienen validez lógica; tales conclusiones son conjeturales, provisionales, hipotéticas y no son predictivas.

3. En la tradición aristotélica, la filosofía utiliza una conceptuación y un vocabulario eminentemente analógicos. En los últimos años, debido al auge de la hermenéutica (interpretación y/o comprensión) del texto, surgió una corriente denominada "hermenéutica analógica": dados dos o más textos se los somete a inspección para ver si, entre ellos, aparecen semejanzas significativas. La hermenéutica analógica se ha desarrollado ampliamente en los estudios religiosos, literarios, jurídicos y filosóficos; por ejemplo, las comparaciones entre los evangelios sinópticos (Mateo, Lucas y Marcos) y el de san Juan han llegado a conclusiones muy interesantes, lo que no implica que tales conclusiones sean

definitivas, pues ya se sabe que todo conocimiento científico es falible; la ciencia, cualquier ciencia, es una "búsqueda sin término", como diría Popper.

4. En la filosofía tradicional suele distinguirse entre "analogía de atribución" y "analogía de proporcionalidad". Hay analogía de atribución cuando se descubren semejanzas entre dos o más sistemas de ideas (códigos, por ejemplo) o también entre dos o más estados de cosas (por ejemplo, dos o más revoluciones políticas). Hay analogía de proporcionalidad cuando se establecen relaciones o correlaciones entre dos o más clases o conjuntos de hechos, por ejemplo, las trayectorias de los planetas alrededor del sol, con las trayectorias de los electrones alrededor del núcleo atómico (modelo de Rutherford-Bohr).

5. Algo muy importante, y que viene desde la época de Aristóteles, es que la analogía o comparación se establece entre palabras o términos, con lo cual todas estas reflexiones adoptan una línea semántica.

El propósito de Aristóteles es mostrar que hay tres tipos de palabras: las unívocas, que tienen siempre el mismo significado; las equívocas, cuyo significado varía según los contextos; y las análogas cuyo significado difiere en parte y en parte coincide. El vocabulario filosófico es esencialmente analógico, por ejemplo en las nociones de ente, verdad, bien, etc. En los dos últimos siglos, la analogía y el método comparativo se han aplicado no sólo al campo de la semántica, sino también a la historia, a las matemáticas, a los textos, a los modelos físicos, etc.

La hermenéutica analógica de los textos, vale decir, su comparación atributiva y proporcional, parece ser el método apropiado de investigación para esta tesis, sin perder de vista lo siguiente: este método no permite hacer predicciones, pues no se puede descartar que en el futuro aparezcan nuevas normas con textos diferentes y hasta contrarios. En las ciencias jurídicas, pero no sólo en ellas, el determinismo causal no es apropiado para la investigación. La hermenéutica analógica permitirá en el desarrollo de esta tesis, el surgimiento de nuevas hipótesis.

1.1.- Hipótesis

Nuestra primera hipótesis postula que para disminuir la lesión al derecho a la intimidad y a la autodeterminación informativa provocada por el procesamiento automatizado de datos personales, es necesario desarrollar una legislación específica de protección de datos personales, que establezca un procedimiento de acceso y rectificación claro junto al control de una autoridad de aplicación especializada, independiente y autónoma del Poder Ejecutivo del Estado.

Si estudiamos el tema de la autodeterminación informativa en el derecho comparado y miramos la hipótesis planteada desde la perspectiva de la legislación europea vigente, puede parecer poco novedosa. Sin embargo, un estudio comparativo de la legislación europea con la normativa del continente americano, nos muestra experiencias y diferencias sustanciales, de las cuales es factible a partir de la demostración o de la frustración de hipótesis, alcanzar un conocimiento científico novedoso para la ciencia del derecho.

Para demostrar el cumplimiento de esta hipótesis procederemos a comparar la legislación de protección de datos personales europea y americana en general y dentro de estos derechos, la legislación española y argentina en particular, para focalizarnos en el problema de las diferencias en las normas y en las experiencias que existen entre estos sistemas jurídicos.

1.2.- Punto de Partida

Al profundizar la justificación de esta tesis, sostenemos que el estudio de la protección de los datos de carácter personal y del derecho a la intimidad nos enfrenta con irrefutables necesidades humanas, hoy amenazadas por la evolución de las nuevas tecnologías de la información y de las comunicaciones.

La penetración tecnológica en la vida de las personas nos plantea un nuevo problema ético y jurídico, ya que el poder sin límites de saber sobre las personas

permite tanto al Estado como al sector privado, acumular y procesar datos personales para hacer, en algunos casos, un ejercicio abusivo de su uso e, incluso un injusto, ilegítimo e ilegal control social sobre ellas.

Los motivos de la acumulación de datos personales pueden ser de interés económico, de estrategia política o militar, de influencia interesada en el consumo de determinados productos o incluso pueden estar originados en una simple curiosidad, lesiva para el desarrollo integral de la persona a quién pertenece esa información. Poder conocer información de otros permite vigilar, controlar, e incluso castigar en forma ilegal, ilegítima y arbitraria[1].

La evolución de una doctrina y de una legislación adecuada en materia de protección de datos personales es hoy necesaria para garantizar la libertad y la autodeterminación de las personas en el siglo XXI. Es, parafraseando a Ihering, una nueva lucha por el derecho.

De allí deriva una importante demanda social del estudio de este problema, al que trataremos de responder, preguntándonos: ¿Es eficaz la protección de los datos personales que realiza el Estado, para proteger la libertad de las personas? ¿Existen organismos de control para la protección de los datos personales que limiten el uso indebido realizado por terceros? ¿Funcionan correctamente? ¿Son independientes del Poder Ejecutivo? ¿Debe esta autoridad de control tener autonomía, autarquía e independencia del Poder Ejecutivo del Estado?

Las respuestas a estas preguntas nos llevarán a determinar las causas o motivos que han impedido a la abundante legislación vigente en materia de protección de datos personales, tanto en Europa como en América, transformarse en una herramienta eficaz de garantía para el derecho a la intimidad de las personas y a su autodeterminación informativa.

[1] Foucault, M. *Vigilar y Castigar. Nacimiento de la prisión*. 16ª reimpresión; 1ª Ed. Siglo XXI Editores. Madrid, 2009, p. 199. La 1ª impresión de esta obra se realizó en Madrid, en el año 1979.

Su conocimiento nos permitirá proponer y proyectar avances a la protección jurídica que deben recibir las personas en lo relativo a sus datos personales, a los efectos de evitar la lesión a sus derechos. El resultado científico busca alcanzar una propuesta de regulación legal más justa y eficaz que la vigente en la materia.

1.3.- Antecedentes

El primer antecedente contemporáneo sobre el derecho a la intimidad fue la publicación del artículo titulado *The Right to Privacy*, en la Revista de la Universidad de Harvard, en 1890. Sus autores, Warren y Brandeis, dieron forma al derecho a "ser dejado solo", del cual toda persona es titular. Esta doctrina, en sus comienzos, estaba pensada solo para determinadas personas que, por ser funcionarios públicos, o por tener una alta exposición pública, o por pertenecer a una determinada clase social, recibían el acoso sin límite de la prensa, aun dentro de los límites de su domicilio particular.

Sin embargo, las bases doctrinarias de la *Privacy*, sin que sus autores pudieran imaginarlo, pronto fueron tomadas para fundamentar el derecho que tienen todas las personas, sin distinción alguna, a proteger su intimidad ante el procesamiento automatizado de datos personales, práctica común, consolidada desde mediados del siglo XX como una actividad en constante aumento.

Seguramente, la proliferación de bancos de datos personales en toda Europa fue el motivo para que en la década de 1970 surgieran las primeras leyes europeas de tutela. La primera de ellas entró en vigencia en el *Land* de Hesse, en Alemania, en el año 1973; le siguieron las legislaciones de todos los Estados miembros de la Unión Europea. Esta institución supranacional, finalmente, promulgó la Directiva Europea 95/46/CE[2], con el fin de armonizar la legislación de toda Europa en materia de protección de datos personales, garantizar su aplicación a todas las personas,

[2] Directiva 97/46/CE. Fci.: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.5-cp--Directiva-97-66-CE-.pdf

pero también buscando no perjudicar la competitividad de las empresas europeas en el mundo.

Las enmiendas constitucionales y las leyes europeas, en especial la legislación española de protección de datos personales, ejercieron una importante influencia en el derecho americano. A fines del siglo XX, esta influencia fue notable en las reformas constitucionales sudamericanas y, más tarde, en las normas de protección de datos personales. Argentina y Chile, entre otros países americanos, han sancionado a comienzos del siglo XXI su legislación de protección de datos personales. Otros Estados de la región todavía debaten proyectos de legislación sobre la materia.

Al finalizar la década del 2010, nos encontramos en Europa con un amplio y profundo desarrollo en su doctrina, en su jurisprudencia y en su legislación de protección de los datos personales. En América, en cambio, el desarrollo doctrinario, jurisprudencial y legislativo está todavía en construcción. Su legislación sigue siendo incompleta y sus instituciones de control de datos personales notablemente frágiles.

2.- Intimidad y procesamiento de datos

No es posible pensar a la humanidad sin su esencial capacidad técnica[3]. El ser humano es poseedor de una inteligencia capaz de descubrir nuevas relaciones entre las cosas que lo rodean, y de esta forma inventa instrumentos y métodos ventajosos para satisfacer sus necesidades[4]. Jorge Saltor afirma que la técnica es incluso anterior a la ciencia porque el hombre se constituye como tal cuando comienza a usar elementos naturales para transformar y mejorar su vida[5], por ejemplo, cuando produce fuego o inventa la rueda.

[3] Saltor J. *La ciencia y el mundo de la vida*. Editorial UNSTA. Tucumán, 2011, p. 204.
[4] Ortega y Gasset, J. *Meditación de la Técnica*. Ed. Revista de Occidente, 3ª edición en castellano, Madrid, 1957, p. 22.
[5] Saltor J. (2011). Op. cit., p. 202.

Al final del siglo XX se han producido cambios importantes que dejaron atrás una etapa de la historia y dieron paso a un nuevo estado caracterizado por la transformación de nuestra cultura, por obra de un nuevo paradigma tecnológico organizado en torno a las tecnologías de la información[6]. Las transformaciones sociales y los cambios generados por las TIC alcanzaron una dimensión de tal magnitud, que para muchos autores pueden ser consideradas una verdadera revolución, al menos tan importante como lo fue la revolución industrial del siglo XVIII.

Las nuevas tecnologías de la información y de las comunicaciones son una consecuencia de esa evolutiva capacidad técnica, creativa, innata en toda persona. Pero a diferencia de otros inventos, las TIC han supuesto una auténtica revolución en el ámbito de los métodos tradicionales de organización, registro y uso de la información, porque permiten almacenar, procesar y transmitir grandes volúmenes de datos, muchos de ellos referidos a todas las personas, sin distinción de ningún tipo[7].

Esta realidad nos lleva a considerar el problema de las conexiones entre intimidad e información en el mundo actual. Indudablemente, la información es poder, y sin ella, ningún gobierno moderno sería capaz de cumplir con sus fines orientados al bien común, pero un uso indebido o abusivo de la tecnología informática de procesamiento de datos, ya sea por parte del gobierno o de determinados grupos privados, afecta al derecho a la intimidad y a la autodeterminación informativa de las personas.

Claro está que a partir de la informática, la información sobre cada persona se compone de datos que ingresan a los sistemas informáticos, se procesan y se

[6] Castells, M. *La Era de la Información. Vol.1.Sociedad en Red*. (Trad. Carmen Martínez Gimeno y Jesús Alborés). 1ª reimpresión; 3ª ed. Alianza Editorial. Madrid, 2008, p. 60.

[7] Por tecnología, Manuel Castells expresa que entiende, en continuidad con Harvey Brooks y Daniel Bell, al uso del conocimiento científico para especificar modos de hacer cosas de una manera reproducible. Y entre las tecnologías de la información incluye al conjunto convergente de tecnologías de la microelectrónica, la informática (máquinas y software), las telecomunicaciones/televisión/radio y la optoelectrónica junto con la ingeniería genética y su conjunto desarrollado de aplicaciones en expansión. Castells, M. (2008). Op. cit., p. 60.

registran en tiempos casi imperceptibles. Sumado a ello, las comunicaciones han alcanzado una gran evolución y desarrollo a partir del siglo XIX. Como resultado, nos encontramos viviendo una era marcada por la revolución tecnológica, en la cual la información sobre las personas puede ser acumulada y transmitida a diferentes puntos del planeta en microsegundos por medio de sofisticadas redes de telecomunicaciones interconectadas[8].

Todos reconocemos que estos avances tecnológicos han mejorado notablemente la calidad de vida de la humanidad y en especial han dado satisfacción a la aparentemente inagotable necesidad de comunicación que reclama la sociedad en la que vivimos. La informática ha avanzado también en forma significativa, optimizando la utilización del tiempo y de los recursos humanos. Sin embargo, debemos tener en cuenta que el tratamiento informático de los datos personales recabados de distintas fuentes permite generar perfiles o imágenes digitales que, además de invadir la vida privada de sus titulares, les impide ejercer un control real sobre esa información[9].

Y aquí surge el conflicto que debe atender el derecho, ante la necesidad que tenemos todas las personas de preservar de un espacio de vida reservado, un espacio de intimidad en el cual las inquietudes, los sentimientos, los pensamientos, las emociones, las pretensiones o cualquier dato en general de cada ser humano requiere ser resguardado para proteger su propia naturaleza.

Las personas han tenido que adaptarse a una sociedad en la que cada vez son más reducidos los espacios privados. Por este motivo, en la actualidad, la lucha por la defensa de la vida privada se ha transformado en la lucha por la defensa y control de la información personal que concierne a cada uno y que revela los comportamientos y hábitos de cada persona, incluso los más íntimos.

---

[8] Estas redes de informática y telecomunicaciones pueden estar conectadas por medio de cables de cobre, líneas de fibra óptica, ondas terrenas o satelitales. Pueden integrar un conglomerado de grandes redes de información, entre las cuales Internet es solo una de ellas.

[9] Davara Rodríguez, M. *La protección de datos en Europa. Principios, derechos y procedimiento*. Ed. Grupo ASNEF EQUIFAX – Universidad Pontificia Comillas de Madrid – ICAI-ICADE. Madrid, 1998, p.11.

Pero ¿cómo hemos llegado a este estado de situación? La revolución tecnológica alcanza una gran aceleración a fines del siglo XIX y continúa sin pausa hasta los tiempos actuales, en los cuales la convergencia e integración digital han permitido una nueva forma de organización social, a la que conocemos como la "sociedad de la información", basada en el conocimiento y en su comunicación. Este proceso de transformación social estuvo acompañado por un discurso que pretendió convertir a la tecnología en un paradigma dominante del cambio y de la garantía de un mundo más solidario, más transparente, más libre e igualitario[10]. Sin embargo, en la contracara de esta nueva forma de convivencia digital, dominante en el siglo XXI, observamos los perjuicios y el daño que la invasión a la intimidad de las personas está produciendo día a día, ante la mirada impotente de millones de damnificados.

La humanidad ha tomado conciencia de la situación de vulnerabilidad en la que se encuentra y ha consensuado límites al derecho a la información mediante el surgimiento del nuevo derecho a la protección de los datos personales sobre el cual pretendemos conocer más en esta tesis.

El tema adquiere interés porque el complejo equilibrio entre estos derechos (información versus autodeterminación informativa) es uno de los más difíciles desafíos de nuestro tiempo. Ambos son derechos necesarios para todas las personas, ambos forman parte del catálogo de los derechos humanos y en muchos Estados, ambos son también derechos fundamentales incorporados en sus constituciones políticas.

En los últimos tiempos fuimos testigos de distintas declaraciones de derechos, diversos convenios internacionales o incluso de enmiendas constitucionales que incorporan nuevas garantías a la protección de los datos personales y en muchos casos cuentan con desarrollos legislativos y reglamentos de protección de datos. Lentamente la doctrina jurídica ha influido para que tanto en

[10] Mattelart, A. *Historia de las Sociedad de la Información*. (Trad. Gilles Multigner). 1ª Edición en la colección de bolsillo. Editorial Paidós. Madrid, 2007, p. 11.

Europa como en América, se sancionen leyes en esta materia. Sin embargo, la intimidad de las personas sigue siendo vulnerada día tras día, sin que todo lo realizado por el derecho hasta este momento haya permitido una real y verdadera protección para los individuos, en lo que respecta a sus datos personales.

Por este motivo, el problema en el cual se enfoca el desarrollo de esta tesis es la protección de los datos personales desde una revisión crítica al tratamiento legislativo dado en Europa y América. El fin es evitar la lesión de los derechos a la intimidad y a la autodeterminación informativa de las personas. Sin embargo, en atención a la amplitud del objeto de estudio, desarrollaremos un análisis especial de la legislación comunitaria europea, americana, española y argentina que se ocupa de este tema. Comparar el marco normativo español y el argentino nos ofrece la ventaja de que ambos derechos participan de un idioma común y de una misma tradición jurídica. Además, al estudiar normativa española, tenemos indirectamente la oportunidad de estudiar también el derecho comunitario europeo, integrador de la legislación de todos los estados miembros de la Unión Europea. Por su parte, el estudio y comparación de la legislación argentina sobre protección de datos personales, nos permitirá analizar una de las legislaciones que probablemente tenga mayor evolución en la región, en esta materia. Esto de ninguna forma significa desconocer la fragilidad institucional de los órganos reguladores o de control de los datos personales que funcionan actualmente en Argentina.

El derecho comparado también nos muestra que, aun cuando el alcance global de la sociedad de la información hace sentir sus efectos en todo el planeta, existen sociedades con mayor evolución tecnológica que otras; y es precisamente en estas donde sus efectos llegaron anticipadamente y donde se ensayaron los primeros remedios jurídicos. Esta realidad permite a la mayoría de los Estados del continente americano, con escasa legislación y jurisprudencia en la materia, tomar la experiencia jurídica europea en la protección de los datos personales para orientarse en seguir sus aciertos y en evitar sus errores. Dar visibilidad a esta situación es uno de los objetivos de estudio que nos motiva y justifica la realización de esta tesis

2.1.- Sobre el concepto de derecho a la intimidad

El punto anterior nos lleva al estudio del derecho a la protección de los datos de carácter personal. Sin embargo, somos conscientes de que al indagar sobre los orígenes de este novel derecho, encontrarnos en el derecho a la intimidad su principal antecedente.

Sobre la relación entre el derecho a la intimidad y el derecho a la protección de los datos de carácter personal surgen algunas preguntas: ¿el derecho a la intimidad es el núcleo del derecho a la protección de los datos de carácter personal? ¿Existe entre ellos una relación de género (derecho a la intimidad) y especie (derecho a la protección de los datos personales)? O bien, ¿el derecho a la protección de los datos personales es una manifestación contemporánea del derecho que todas las personas tenemos a proteger nuestra intimidad y nuestra vida privada?

De estos interrogantes, que surgen de forma espontánea, nos queda claro que nuestro punto de partida en el estudio del derecho a la protección de los datos debe ser el concepto de derecho a la intimidad. Al respecto Emilio Suñé Llinás nos recuerda que el derecho a la intimidad es un derecho que se ha configurado en tiempos relativamente recientes, en términos históricos. Se presenta como un derecho fundamental diferenciado, dado su vínculo con la tecnología; y para fundamentar esta afirmación, Suñé Llinás, nos recuerda el punto de referencia inicial del derecho a la intimidad es la obra de los autores Warren y Brandeis publicada en el año 1890 con el título *The Rightto Privacy*. Explica que esta obra fue escrita como consecuencia de las nuevas posibilidades que la tecnología comienza a dar a la prensa para captar y almacenar imágenes fotográficas y sonidos a fines del siglo diecinueve[11].

[11] Suñé Llinás, E. *Tratado de Derecho Informático. Volumen I: Introducción y Protección de Datos Personales.* Segunda Edición (Actualizada por Cristina Almuzara Almaida). Editorial Servicio de Publicaciones Facultad de Derecho de la Universidad Complutense de Madrid. Madrid, 2002, p. 37.

Su evolución histórica será un peldaño ineludible para intentar comprender el problema que nuevas tecnologías de la información y de las comunicaciones, presenta para la necesidad humana de mantener alguna reserva de los datos personales que conciernen a cada persona.

La ciencia del derecho se encuentra en el siglo XXI, ocupada en proteger los derechos humanos en general, y entre ellos, el derecho a la autodeterminación informativa, como un nuevo derecho humano de tercera generación, que se presenta como una extensión del derecho a la intimidad. Suñé Llinás destaca que la intimidad es un derecho reciente en términos históricos, sobre el que no se ha puesto suficientemente de relieve que su nacimiento mismo como Derecho Fundamental diferenciado está vinculado a la tecnología y, en el fondo, siempre fue autodeterminación informativa[12].

En términos históricos, el derecho a la intimidad se configuró en tiempos recientes como un derecho autónomo desgajado del derecho al honor. El vocablo intimidad alude al carácter oculto o secreto de aquellas circunstancias que rodean la existencia del hombre, pero también se refiere a circunstancias internas, esenciales del individuo, que hacen al núcleo o centro de su personalidad. En este sentido, el Diccionario de la Real Academia de la Lengua Española define "intimidad" como "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia"[13]. Otra definición acuñada por la doctrina es aquella que la describe como "el derecho del individuo a decidir por sí en qué medida o en qué circunstancias desea compartir con terceras personas sus pensamientos, sentimientos y expresiones personales"[14]. Se destaca en esta última definición la

[12] Ibídem.
[13] *Diccionario de la Lengua Española*. Real Academia Española. Ed. Espasa-Calpe, Madrid, 2006. Sitio Web de la Real Academia Española: En Internet*: Diccionario de la Lengua Española*, Vigésima Segunda Edición: http://lema.rae.es/drae/ (último ingreso: 21/07/2012).
[14] Herrán Ortiz, A. *La violación de la intimidad en la protección de datos personales*. Editorial Dykinson, Madrid, 1998, p 2.

acción de "decidir por sí", ya que decidir implica ser libre[15] y en este punto se observa con claridad la directa conexión entre intimidad y libertad.

Intimidad se refiere a la esfera en la cual se desarrollan las facetas más reservadas de la vida de una persona. Pero en nuestra exploración buscamos encontrar una relación conceptual que nos permita dar fundamento a un derecho amplio a la protección de los datos personales. Inmediatamente aparece como opción el término "privacidad", al cual llegamos traduciendo desde el inglés, probablemente sin precisión, la palabra *privacy*[16], integrante del título de la obra doctrinaria que figura como el antecedente más importante en esta materia: el artículo titulado *The Right to Privacy*[17], escrito por los juristas Samuel Dennis Warren y Louis Dembitz Brandeis, doctrina de la cual nos ocuparemos más adelante.

Al momento de buscar antecedentes del derecho a la intimidad en la *privacy* anglosajona, observamos que el término privacidad fue incorporado por la Real Academia Española como un vocablo castellanizado, recién a partir del año 2001, en la Vigésima Segunda edición del Diccionario de la Lengua Española. Es decir que hasta el año 2001 el vocablo privacidad fue una palabra extraña al idioma castellano[18], y recién con posterioridad fue definido en el diccionario de la Real Academia Española como "Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión"[19].

---

[15] Zapater Carón, J. *La libertad en Karl Jasper*. Editorial Librería General. Zaragoza, 1981, p. 60.
[16] En la lengua inglesa la palabra *intimity* se suele emplear para denominar las relaciones sexuales ilícitas, por lo que es conveniente evitar su uso para el objeto que aquí estudiamos. Queda entonces, en el idioma inglés, solo la palabra *privacy* para designar tanto "intimidad" como "vida privada".
[17] Warren, S.D.; Brandeis L.D. "The rigth to the privacy". Volumen IV, nº 5 de 1890, en Harvard Law Review; pp. 193-219.Traducción al castellano de Benigno Pendás y Pilar Baselga, publicada con el título Derecho a la Intimidad. Ed. Civitas. Madrid, 1995.
[18] *Diccionario de la Lengua Española*. Real Academia Española. Vigésima Primera Edición. Ed. Espasa-Calpe, Madrid, 1992, p. 1669 (ir a esta página para observar que en esa edición el término privacidad todavía no figuraba. Recién fue incorporado en la 22ª Edición).
[19] *Diccionario de la Lengua Española*. Op. cit., p. 1183.

La lengua inglesa tiene dos términos de parecido significado en su vocabulario[20], pero los autores mencionados, al momento de darle nombre al derecho que estaban fundando en su precursor artículo, se inclinaron por el de privacidad. Otras lenguas usan palabras diferentes para expresar el contenido de los términos intimidad y privacidad[21]. Por este motivo, la opción correcta sería usar, en nuestro idioma, con una diferencia de menor y mayor alcance, los términos "intimidad" y "vida privada"[22]. Este último término define un conjunto, más amplio y más global, de facetas de la personalidad de una persona que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente relacionadas entre sí, nos arrojan una imagen de esa personalidad que su titular tiene derecho a mantener en reserva. En consecuencia, observamos que si el derecho aún no le ha dado una protección suficiente a la intimidad, en su sentido estricto, menos ha hecho por la protección de la vida privada.

Mientras el *Diccionario de la Lengua Española* define "intimidad" como una zona espiritual y reservada de una persona o de un grupo, especialmente de una familia[23], sobre la palabra "privada"[24], en sus diferentes acepciones da como significado "que se ejecuta a vista de pocos, familiar o domésticamente, sin formalidad ni ceremonia alguna, particular y personal de cada uno". Por último, recién en la 22ª edición de 2001, define privacidad como "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".

Está ampliamente reconocido en la doctrina y en la jurisprudencia[25] que el derecho a la intimidad como concepto jurídico nació en los EEUU a partir de un

---

[20] *Privacy; Intimity*

[21] En alemán: *Intimitäty Privat Leben*; en francés: *Intimité* y *vie privée*; en italiano *intimitá* y *riservatezza*; en inglés: *intimity* y *privacy* y en español sería intimidad y vida privada.

[22] Del Peso Navarro, E; Ramos González, M. *Confidencialidad y Seguridad de la Información: La LORTAD y sus implicaciones socioeconómicas*. Editorial Díaz de Santos. Madrid, 1994, p. 63.

[23] Diccionario de la Real Academia de la Lengua Española. Op. cit., p. 835.

[24] Ibidem, p. 1.183.

[25] Sentencias de todo el mundo citan el artículo "The Right to Privacy" de Samuel D. Warren y Louis D. Brandeis, a modo de ejemplo mencionamos el voto del Dr. Carlos Fayt, en el importante fallo del caso Ponzetti de Balbin c/ Editorial Atlántida, pronunciado por la Corte Suprema de Justicia, 1982 (Argentina), en el cual se sientan las bases del derecho a la intimidad y a la propia imagen.

artículo publicado por dos abogados en una revista jurídica de la Universidad de Harvard el 15 de diciembre de 1890. Samuel D. Warren y Louis D. Brandeis titularon a su ensayo "El derecho a la privacidad" (*The Right to Privacy*)[26].

La obra responde a una inquietud del propio Samuel Dennis Warren, abogado. Los autores eran dos abogados que habían sido compañeros de promoción en la *Harvard Law School* donde se graduaron en los dos primeros puestos, en el año 1877. Dos años más tarde formaron un estudio jurídico en Boston al que denominaron Warren & Brandeis abogados.

En 1884, Warren se casó con Mabel Bayard, hija de un senador, miembro de la clase social más distinguida de Boston. Mabel Bayard tenía por costumbre ofrecer fastuosas fiestas que interesaban mucho a la prensa de Boston, en particular al semanario *Saturday Evening Gazette,* que cubría la noticia con detalles que irritaron profundamente a Warren y llevaron su atención sobre la legitimidad o ilegitimidad de tales informaciones. Este hecho social fue la causa directa que llevó a los autores a escribir, luego de seis años de estudio, sobre el derecho a la privacidad junto con su compañero y socio Brandeis (más tarde juez del Tribunal Supremo de los EEUU)[27].

En esos tiempos el peligro para la vida privada no era la informática, si lo era la prensa. Los autores buscaban, con el artículo mencionado, proteger a las personas de la intromisión de la prensa en sus vidas privadas, nunca pensaron en construir un derecho común a todas las personas, por el sólo hecho de serlo, sin distinción de clases sociales, capacidad económica, función pública o privada, ni de ningún tipo. Por el contrario, pensaban que estaban prestando servicios intelectuales a la formación de un derecho solo para los funcionarios públicos y personas de alta exposición o reconocimiento público. Sin saberlo, habían elaborado una nueva

[26] Warren, S.; Brandeis, L. "The Right to Privacy". Vol. 4, N° 5, Harvard Law Rev (Revista Jurídica de la Universidad de Harvard). Cambridge, Massachusetts (EEUU), 1890, p. 193. Fci.: http://www.law.louisville.edu/library/collections/brandeis/node/225

[27] Urabayen, M. *Vida Privada e Información*. EUNSA (Ediciones de la Universidad de Navarra S.A.). Zaragoza (España), 1977, p. 90.

doctrina que más tarde se aplicaría para proteger a todas las personas por igual, sean funcionarios públicos o no, sean personas de alta exposición pública o personas retiradas del escenario público, etc. Estaban construyendo una doctrina para la defensa de todas las personas.

El concepto de intimidad está todavía lejos de haber sido definido con claridad por su naturaleza evolutiva y su condicionamiento histórico, social y tecnológico. El concepto de vida privada es de mayor utilidad para fundamentar el derecho a la protección de datos, ya que, desde la amplitud de su definición, podemos fundamentar una protección a los datos referidos a una persona, (su titular), incluyendo aspectos o datos que individualmente no tienen mayor trascendencia; pero que al unirlos a otros pueden configurar un perfil determinado sobre un individuo, cuya protección y reserva tiene derecho a exigir[28].

Pérez Luño entiende que conviene configurar una definición que sea apta para ofrecer un marco unitario al tratamiento los problemas conexos con el aumento de la información que se puede disponer acerca de una persona[29]. Coincidimos con el autor citado en la necesidad de alcanzar una definición que sea útil para desarrollar una serie de garantías jurídicas que eviten la intromisión en la vida privada por medio de tecnologías que ofrezcan perfiles detallados de una persona y vulneren sus derechos humanos a la intimidad y a la protección de sus datos personales.

La protección de los datos de carácter personal es resistida por sectores interesados en almacenar datos personales y usarlos de diferentes formas: para controles abusivos de los gobiernos y aparatos estatales que acumulan información con la intención de manipular a los titulares de esos datos, con la egoísta intensión de conservar su poder, proteger intereses comerciales del mundo empresarial u otras

[28] Davara Rodríguez, M. "La ley española de protección de datos (LORTAD): ¿una limitación al uso de la Informática para garantizar la intimidad?". Revista Actualidad Jurídica N° 76, Editorial Aranzadi, Pamplona, 12 de noviembre de 1992.
[29] Pérez Luño, A. *Derechos Humanos, Estado de Derecho y Constitución*. Editoriales Tecnos. Madrid, 1984, p. 329.

causas que, bajo la aparente vocación por el progreso y la investigación científica, violan derechos humanos esenciales.

Arnold Toynbee explica que una sociedad crece cuando da respuesta a una determinada incitación o desafío. Esa generación, nos dice Toynbee, no solo es triunfante en sí misma, sino que además provoca otra incitación, que en las sociedades en evolución encuentra a su vez otra respuesta triunfante. En cambio, si la sociedad no supera ese nuevo desafío se estanca.

Las nuevas tecnologías de la información y de las comunicaciones actúan como una incitación al crecimiento de nuestra sociedad de la información, y para no estancarnos, debemos responder garantizando el equilibrio entre el derecho a la información y el derecho a la intimidad de las personas.

Toynbee sostiene que "el progreso de una civilización consiste en un proceso de superación de obstáculos materiales que permiten que las energías de la sociedad den respuesta a incitaciones que son internas antes que externas y espirituales antes que materiales"[30]. El derecho a la intimidad es una necesidad interna y espiritual de las personas, que opera ante la adversidad del mundo civilizado de nuestro tiempo. Responder con éxito a esta incitación o fracasar en la respuesta, será un indicador del crecimiento o estancamiento de nuestra civilización.

La información siempre fue valiosa, pero las nuevas tecnologías de la información y de las comunicaciones le dan hoy una nueva dimensión, un nuevo valor que antes no tenían porque no existía la posibilidad de convertir datos parciales y dispersos, en información de masas, científicamente organizada.

La información tiene un valor importantísimo para el poder del Estado moderno. La tierra, el trabajo, el capital, los recursos naturales o la acumulación monetaria han pasado a un segundo plano, detrás del poder informativo, para el Estado del siglo XXI. Hoy el poder está en la información y el conocimiento. Por

[30] Toynbee, A. *Estudios de la Historia*. Compendio IX/XIII (Tomo 3). Sexta re-impresión. Editorial Alianza. Madrid, 1991, p. 339.

ello el sistema jurídico debe ejercer un control adecuado que garantice la seguridad jurídica que todo Estado de derecho debe tener, sin descuidar la protección de los derechos humanos a todos sus habitantes

Con la finalidad alcanzar el bienestar general de la población, el Estado interviene en ciertos sectores de la estructura social, se relaciona con los administrados y participa de una nueva economía basada en el conocimiento[31]. A tales efectos, los gobiernos almacenan y clasifican datos personales, los valoran y los utilizan en su accionar político y administrativo cotidiano. Los sistemas informáticos actuales tienen una gran capacidad y velocidad de almacenamiento de datos personales[32]. Sin embargo, junto a estos importantes avances aportados por la tecnología informática, también surgen serias amenazas para los derechos y libertades de los individuos. Estos riesgos son especialmente peligrosos en el caso de la intimidad.

La sociedad tecnológicamente desarrollada cuenta con los medios para registrar la formación escolar y universitaria, las operaciones financieras, la trayectoria profesional, los hábitos de vida, el historial clínico, las creencias religiosas, políticas o gremiales de las personas, en archivos capaces de ser cruzados en una red general de información. Las personas van dejando tras su trabajo, su ocio, o los servicios de los que se sirven, innumerables datos acerca de su personalidad. En cada ocasión en la que proporcionan su filiación, domicilio, experiencia profesional, datos bancarios o antecedentes médicos, contribuyen a engrosar los archivos automatizados de datos que van aumentando el volumen de

[31] Toffler, A. *El Cambio del Poder*. (Trad.Rafael Aparicio). Plaza y Janes Editores S. A., 4ª edición. Madrid, 1995, p.p. 426-430.Titulo original de la obra: *Power Shift*.

[32] Ya en 1974, IBM ofrecía equipos capaces de almacenar hasta cuatrocientos setenta y dos millones de bytes. Esta cifra se corresponde con el contenido de diecinueve millones de páginas escritas a máquina, que sería el contenido de una biblioteca de treinta mil libros, por un promedio de quinientas páginas por volumen. En cuanto a la gran velocidad de trabajo, el citado sistema de memorización de IBM podía tener a disposición la información almacenada de ocho a trece segundos. Téngase en cuenta la fecha a la que estamos haciendo referencia, en la cual se usaban equipos informáticos de tercera generación, desarrollados entre los años 1965 y 1976, actualmente los sistemas informáticos en red ofrecen posibilidades de almacenamiento de información muy superiores.

información, en directa proporción a la disminución del grado de reserva o intimidad de sus vidas privadas[33].

El problema planteado se agrava si tomamos en cuenta que el Estado no es el único actor, sino que junto a él también actúa el sector privado a través de pequeñas, medianas y grandes empresas. Este sector también ha incorporado tecnología de la información y de las comunicaciones para el logro de sus fines y objetivos.

La revolución de las tecnologías de la información y las telecomunicaciones ha planteado al mundo contemporáneo un nuevo problema. El fenómeno informático invade no solo la esfera pública, sino también la privada; tanto la Administración Pública como el sector privado se valen del soporte informático para la adquisición, valoración y utilización de informaciones que unas veces les permiten cumplir con sus fines y objetivos y otras extralimitarse en el uso de la información que tienen en su poder.

Debemos agregar que la conectividad o comunicación de las diferentes redes de datos es un agravante, ya que genera más peligro de lesión al derecho a la intimidad de las personas. El cruce de información permite trazar con facilidad un detalladísimo perfil de cada individuo[34]. De esta forma la tecnología deja de ser una herramienta al servicio de la humanidad para transformarse en un instrumento de poder que amenaza y vulnera tanto al derecho a la intimidad del individuo como a otros derechos y libertades indisolublemente ligados a él.

Surgen así nuevas asimetrías en las relaciones entre los ciudadanos y los poderes públicos y privados. La acumulación de grandes cantidades de información que afectan a la intimidad de las personas, ha generado un nuevo tipo de dominio, desconocido hasta no hace mucho tiempo.

---

[33] Frixes San Juan, T. *Obtención y utilización de datos personales automatizados*. Jornadas sobre derecho español de la protección de datos personales. Registro General de Protección de Datos de Madrid, 1996, Publicación en CD-ROM.

[34] Zavala de González M. *Derecho a la Intimidad*. Ed. Abeledo-Perrot. Buenos Aires, 1982, p. 13.

Nuestras sociedades informatizadas del siglo XXI se estructuran sobre un poder que ya no reposa solo en el ejercicio de la fuerza física, sino también en el uso de la información para el control de las conductas de los ciudadanos[35].

De todas formas, aun cuando el Estado moderno debe buscar la forma de obtener el máximo provecho de las nuevas tecnologías de la información y de las comunicaciones, y definir políticas de distribución de esa información y conocimiento. Debe buscar un equilibrio en el cual el ideal democrático de la libertad de expresión no se transforme en una prioridad que aplaste al derecho a la intimidad y a la autodeterminación informativa que toda persona necesita para el desarrollo integral de su personalidad.

También es cierto que ninguna sociedad puede tolerar una libertad de información total, ya que la vida social requiere algo de secreto, algún espacio donde se preserve una zona de reserva para la intimidad individual. La libertad de información total no es más permisible que cualquier otro derecho en su dimensión absoluta.

Por estos motivos antes mencionados, Suñé Llinás nos explica que el derecho a la intimidad ha evolucionado en la dirección de tres vectores diferentes[36]:

a) El primer vector sigue una dirección que busca alcanzar a una mayor cantidad de personas. Inicialmente responde a la inquietud de un grupo minoritario perteneciente a una clase acomodada que es asediada por la prensa. Sin embargo, posteriormente la evolución del derecho a la intimidad, en esta dirección o vector, va a lograr alcanzar a todas las personas, con independencia de su pertenencia a una clase social o no. Es decir que llega a otras capas sociales,

[35] Lozano, M.; Pérez Luño, A.; Guerrero Mateus, M. *Libertad informática y leyes de protección de datos personales.* Publicado en Cuadernos y Debates. Publicación del Centro de Estudios Políticos y Constitucionales de Madrid (ISBN: 84-259-0841-8). Madrid, 1989, p. 30.
[36] Suñé Llinás, E. *Tratado de Derecho Informático. Volumen I: Introducción y Protección de Datos Personales*. Op. cit. (2002), pp. 38-39.

b) El segundo vector evoluciona en la dirección de la autonomía del Derecho a la intimidad, que actualmente es pacíficamente reconocida por la doctrina como un derecho que no se separa completamente de otros derechos, tanto o más fundamentales (entre ellos el derecho al honor y a la dignidad de las personas) pero que a pesar de ello, adquiere autonomía y características que le son propias.

c) El tercer vector sigue la dirección de la evolución tecnológica, dado que tanto la jurisprudencia como la doctrina que se ocupó del tema, reconoce el vínculo que existe entre el derecho a la intimidad y las nuevas posibilidades que ofrecen las TIC para invadir las zonas de reserva de una persona. En otras palabras, existe una relación de proporcionalidad paralela: a mayor evolución tecnológica, es necesaria una mayor protección jurídica del derecho a la intimidad, hoy configurado como un derecho que adquiere una nueva dimensión a la que llamamos autodeterminación informativa por sus particulares características en tiempos de las TIC.

Como podemos observar, el derecho a la intimidad tiene fronteras conceptuales propias y por ello puede ser reconocido como un derecho autónomo que se caracteriza por su enorme flexibilidad e imprecisión conceptual. Pero es necesario reducir al mínimo tal imprecisión conceptual existente en el término y sus consecuencias; ya que el ámbito de cobertura de un derecho equivale a todo su ámbito conceptual integrado por aquellas situaciones sobre las que es llamado a actuar.

Esto nos lleva a la necesidad de determinar qué situaciones quedan dentro de su ámbito de cobertura y cuáles fuera de él. Es necesario encontrar el equilibrio entre el derecho a la intimidad y el derecho a la información, mediante instrumentos jurídicos que garanticen el ejercicio de ambos derechos.

2.2.- Diferencias con otras manifestaciones de la personalidad

Ya expresamos que, a nuestro entender, para realizar una investigación jurídica sobre la protección de datos, es necesario primero abordar el concepto de derecho a la intimidad, considerado núcleo desde el cual nace y evoluciona el nuevo derecho a la protección de datos personales hasta alcanzar autonomía.

La idea de intimidad se confunde con otros conceptos que tienen en común la proximidad con la zona de reserva de toda persona. Por este motivo, necesitamos delimitar el concepto y despojarlo de aquellas expresiones o realidades que lo confunden. Establecer una delimitación conceptual contribuye en gran medida a esclarecer lo que se entiende por intimidad y así observar la relación con el concepto de datos personales.

Un mismo dato, pensamiento o sentimiento puede ser íntimo, secreto o confidencial, por las circunstancias que deciden a la persona, a reservarlos[37].

2.2.1. Lo confidencial

Abarca un ámbito especial de reserva que, a diferencia del concepto de intimidad, actúa como un instrumento que el individuo utiliza según los fines que tenga en mente. Son los pensamientos, sentimientos, datos o informaciones íntimas o que se resguardan en la zona de reserva de una persona, que luego decide revelarlos a otra, esperando que no los difunda o divulgue a los demás. Los datos confidenciales tienen la particularidad de haber sido obtenidos de alguien que no autoriza a utilizarlos hasta tanto se cumplan determinadas condiciones o circunstancias. La diferencia con el dato secreto radica en la relación de confianza que hay entre el titular, confidente o divulgante del dato y el receptor del dato. Es patente la derivación del término confidencial, de la palabra confianza. A modo de ejemplo podemos proponer como confidencial la conversación entre un laico católico y un sacerdote en el marco del sacramento de la confesión.

[37] Herrán Ortiz, A. (1998). Op. cit., p. 12.

2.2.2. Lo secreto

Lo secreto implica ausencia de información sobre la vida de una persona. Es decir que lo secreto hace referencia a una observación que se percibe desde fuera de la persona, desde una posición externa a su zona de reserva. Lo secreto veda a los demás el acceso a esos datos o informaciones, implicando, para quien tiene acceso a ellos, una obligación o deber de ocultarlos. A diferencia del dato confidencial, en el dato secreto parece haber más una relación de obligación que de confianza. Se ha entendido habitualmente que el concepto de secreto mantiene una intensa vinculación con aquello que cada persona se guarda para sí, con la intención de no revelarlo a los demás. Si un pensamiento, sentimiento o comportamiento es secreto, significa que está oculto, que no se encuentra expuesto a la curiosidad ajena. La naturaleza de la información o del bien u objeto ocultado, no es una cuestión de interés para establecer el secreto. Puede serlo cualquier conducta, acto, documento, sentimiento o relación que la persona a quien afecte desee preservar del conocimiento externo, sin que necesariamente tenga que formar parte del interior o de la esencia de la personalidad de un individuo. A modo de ejemplo podemos decir que la información sobre el estado de salud del Presidente venezolano Hugo Chávez en enero de 2013 era información secreta.

2.2.3. Lo íntimo

Lo íntimo se refiere a una esfera tan interior del individuo, que, en principio, solo él puede revelar. No consiste en la ausencia de información personal sobre una persona y por ello, sería desacertado considerar que cuanto menos se conozca de la vida de una persona, ella goza de mayor intimidad. La intimidad no es sólo ausencia de información personal, ya que incluye aquello que cada persona se reserva para sí, haciendo ilícito a los demás su penetración o invasión.

Se diferencia de lo confidencial porque este tipo de información es aquella que el interesado revela a alguien con la intención o el ánimo de que no sea develado a los demás sin su consentimiento. De igual manera, al diferenciar lo

íntimo de lo secreto, observamos que la intimidad no implica exclusivamente la ausencia de información sobre la vida de una persona; representa, por el contrario, una necesidad de "vida interior" o relación intra-personal, de reflexión sobre sus propios pensamientos y sentimientos.

Puede ser frecuente que terceros ajenos al individuo dispongan de concretas informaciones que atañen a la vida y personalidad de una persona, obtenidas para fines y objetivos determinados que, sin embargo, no los habilitan a emplearlos con propósitos diferentes.

Mientras la intimidad faculta al individuo a practicar un control eficaz sobre sus propias experiencias y vivencias, la confidencialidad constituye un medio o instrumento de protección de esa intimidad. En esta línea, la intimidad no es una cuestión de ocultamiento o secreto, que corresponda a terceros en atención a las circunstancias que justificaron la revelación, sino de una libertad del individuo que este necesita para disponer plenamente de su vida y de su personalidad.

Concluimos que la intimidad queda lesionada mucho más por el ataque a la libertad interior del sujeto que por la difusión que se dé a determinados datos referidos a una persona. La violación de la intimidad implica el desconocimiento de una libertad interna, necesaria para el desarrollo de una persona.

La confidencialidad representa una manifestación de la confianza que se ha depositado en un tercero, que será quien oculte, con la complicidad del sujeto titular de la información, lo que le ha sido revelado. Consiste en una exteriorización de los comportamientos y actitudes como expresión de las propias relaciones humanas, si bien con la garantía y el compromiso de que lo que se ha compartido no será expuesto al conocimiento general.

La intimidad constituye la máxima expresión de la interioridad humana, de relación con uno mismo. Es necesaria para el autoconocimiento y el desarrollo de un mundo íntimo y propio, que por su esencia es un derecho humano que tenemos todas las personas y que a nadie le es lícito invadir. La intimidad representa una

vida interior, un desarrollo personal e intelectual que está más allá del ocultamiento o aislamiento. La intimidad es vulnerada cuando al individuo se le niega toda posibilidad de vida interior[38].

En conclusión, intimidad y vida interior se implican una a otra; de hecho Warren y Brandeis hacen referencia a ambos términos en su artículo citado *The Rightto Privacy*; los dos juristas norteamericanos emplean la expresión "intimidad de la vida privada" que será utilizada ochenta años después por la ley francesa de 1970 al introducir el artículo 9 del Código Civil[39].

Por lo ya expresado, lo íntimo y lo secreto son conceptos que se identifican, aun cuando sea frecuente que aquello que la persona quiere ocultar, guarde profunda relación con lo que para ella representa la parte más íntima o la esfera más significativa de su persona. No se halla unida, por tanto, la condición de secreto con la de íntimo; claro que son conceptos que se complementan porque pueden aplicarse y de hecho se aplican a realidades diferentes. A modo de ejemplo podemos mencionar información que comparte el médico y su paciente. No todo lo secreto o confidencial será íntimo. Aquello que es revelado en determinadas circunstancias a determinadas personas, aunque no se identifique con la interioridad del individuo ni con su esencia personal, deberá ser ocultado por aquellos a quienes se comunicó en forma confidencial o para su secreto. Es decir, que quienes recibieron esta información tienen el deber jurídico o moral de no compartirla con terceros ni con extraños.

Si nos centramos en explicar la obligación del secreto en la correspondencia y en las comunicaciones, podemos comprender la esencia y sentido de esa obligación, aun cuando el contenido de la información o documentación que se comunica o envía, nada tenga que ver con la intimidad de una persona. Poco importa que lo expresado en una carta o en una conversación telefónica afecte a la

[38] Orwell, G. *1984*. (Trad. Rafael Vázquez Zamora). Editorial Austral, Ediciones Destino. Madrid, 2010, p. 35. (1ª ed.1966).
[39] Urabayen, M. *Vida Privada e Información. Un conflicto permanente*. EUNSA (Ediciones de la Universidad de Navarra S.A.). Zaragoza (España), 1977. p. 93.

más profunda esencia del individuo o se trate de una información intranscendente; todo ser humano, como manifestación de su dignidad, y como instrumento garantizador de su libre desarrollo personal e intelectual, precisa que aquello que comunica o comparte con otros permanezca reservado y no trascienda al conocimiento general. Esta garantía representa una legítima aspiración humana que permite una libre actuación individual, al tiempo que asegura el respeto a los derechos personales más significativos del individuo, tales como la libertad de relación con los demás o la reserva de su vida privada.

El deber de secreto constituye una de las manifestaciones del derecho a la intimidad[40], pero no se confunde con él. En ocasiones, el deber de ocultar se limitará a bienes de la personalidad, a la esfera interior de la persona, pero la mayoría de las veces lo que se debe reservar del conocimiento ajeno serán informaciones no íntimas, por ejemplo informaciones de tipo económico o patrimonial; sin embargo, también estas informaciones constituyen el contenido del deber de secreto. Así, lo íntimo es lo más personal, siendo, por tanto, todo lo íntimo secreto y reservado. Representa, por otro lado, una evidencia que cada persona puede desvelar por decisión propia.

En general, en el derecho comparado, la legislación ha evitado ofrecer un concepto claro y preciso de intimidad, susceptible de delimitar la extensión o contenido de esta, frente a otras realidades afines, como la vida privada o el secreto.

Por el contrario, la legislación española, en algunos casos, ha aumentado la confusión. Esto sucede con el artículo 2 (1) de la Ley Orgánica 1/82[41], al expresar que "*tal delimitación habrá de tener lugar no solo por las leyes sino también por los usos sociales, atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí o para su familia*"[42]. La remisión del concepto en la

[40] Herrán Ortiz, A. (1998). Op. cit., p. 15.
[41] Ley Orgánica 1/82 (España), de 5 de mayo, sobre derecho al honor, a la intimidad personal y familiar y a la propia imagen. Publicada en el BOE del 14 de Mayo de 1982.
[42] Artículo 2 (1) de la Ley Orgánica 1/82 (España). Fci. : http://www.boe.es/aeboe/consultas/bases_datos/doc.php?coleccion=iberlex&id=1982/11196, Boletín Oficial del Estado, España (último ingreso: 3 de diciembre de 2009).

normativa de protección de datos personales a otras leyes vigentes[43], además de ser ineficaz para configurar un concepto de intimidad que sirva de referencia, solo sirve para aumentar la confusión mediante una permanente remisión de una ley a otra ley, y así sucesivamente.

El silencio o las confusas remisiones en materia de derecho a la intimidad, debieron ser resueltas, en ese orden jurídico, por la jurisprudencia española que, a través del Tribunal Supremo, declaró que "la delimitación de la esfera de la intimidad es eminentemente relativa y ha de ser el juzgador quien, en referencia a cada persona, y atento a las circunstancias del caso, prudentemente, delimite el ámbito de la protección"[44].

En consecuencia, desde un análisis crítico pensamos que la intimidad es un derecho innato en cada persona, que surge desde el comienzo de su vida y se encuentra inserto en su naturaleza humana. En lo íntimo está presente tanto el interés del individuo, de la persona en cuanto tal, por ser respetada en aquello que desea reservar para sí o que solo quiere compartir con un círculo restringido, como también, y principalmente, el interés de la sociedad a que ello suceda así, pues al fin y al cabo, lo que subyace bajo este derecho es precisamente la libertad humana, configurada como un fundamento del orden político y de la paz social.

2.2.4.- Honor y propia imagen

Tanto el derecho a la intimidad como el derecho a la protección de los datos de carácter personal tienen semejanzas con los derechos al honor y a la propia imagen, ya que todos ellos son derechos, universales e imprescriptibles.

---

[43] Cabezuelo Arenas, A. *Derecho a la Intimidad*. Editorial Tirat lo Blanch, (Tirant, monografías n° 96), Valencia, 1998, p. 19.

[44] STCE (España), Sala Civil, 4 de Noviembre de 1986.
fci.:
http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=1167504&links=la%20delimitacion%20de%20la%20esfera%20de%20la%20intimidad&optimize=20051011

Se fundamentan en la noción de persona, en su naturaleza humana y por lo tanto son también derechos innatos y naturales a todo individuo. Una posición en contrario implicaría negarles la condición de derechos universales[45].

Los fundamentos mencionados junto con el contundente desarrollo del derecho internacional en la materia impiden al derecho positivo interno la posibilidad de desconocer estos derechos. En otras palabras, estos derechos de la persona no pueden ser restringidos por cuestiones raciales, económicas o de cualquier otra índole que el derecho positivo de un Estado contemple en su ordenamiento.

Aun así, entre el derecho a la protección de los datos de carácter personal, el derecho al honor[46] y a la propia imagen[47], hay marcadas diferencias.

La diferencia principal entre el derecho a la protección de los datos de carácter personal y el derecho al honor radica fundamentalmente en que el primero de estos derechos otorga a toda persona la facultad de tomar conocimiento de los datos a ella referidos y de solicitar la eliminación, rectificación, confidencialidad o actualización a la base de datos. En cambio, el derecho al honor se detiene a observar el estado de la reputación de una persona y a protegerla, evitando la difusión de toda información que la deteriore. Mientras el derecho a la protección de datos personales busca proteger la posibilidad de autodeterminación que debe tener toda persona, el derecho al honor busca proteger su reputación.

A diferencia del derecho a la protección de los datos de carácter personal y del derecho al honor, el derecho a la imagen, en cambio, se limita a proteger los documentos o datos que dan cuenta de la imagen de una persona. Este instituto no atiende a la reputación, al honor ni a la autodeterminación informativa de la persona. Por el contrario, sólo se ocupa de determinar a quién pertenece la imagen y

[45] Finnis, J. (1984). *Natural Law and Natural Rights*. (2ª Edición) Editorial Oxford UniversityPress, Nueva York. 2011, p. 225.
[46] Rebollo Delgado, L. *El derecho fundamental a la intimidad*. Editorial Dykinson (2ª Edición Actualizada). Madrid, 2005, p. 26.
[47] Ibidem, p. 44.

a otorgar a su titular el derecho a reclamar por el uso de su imagen, sin su autorización.

Notamos entonces que al analizar el alcance de la protección que corresponde al derecho al honor, es necesario tomar en cuenta los actos propios del afectado junto con los usos y costumbres en la materia, para poder conocer cuál es la reputación que a ese individuo le corresponde defender.

No sucede lo mismo con el derecho a la propia imagen ni con el derecho a la protección de los datos personales. En caso contrario, estaríamos construyendo estatutos de derechos diferentes para cada persona. Y en lo que atañe a los datos de carácter personal, llegaríamos al absurdo de construir un derecho con contenido cambiante y diferente, según fuere el sujeto respecto del cual se predique. Si para configurar el contenido de este derecho fundamental atendiéramos a los propios actos realizados por la persona afectada, correríamos el riesgo de privar injustamente de dicho derecho a quienes no hubieren actuado con una actitud reservada en tiempos anteriores al hecho lesivo a su intimidad. Una conclusión de esta naturaleza sería, a nuestro entender, absurda, dado que quienes antes hicieron concesiones en este plano y proporcionaron algunos de sus datos personales a terceros, no por ello renunciaron al derecho a su intimidad y a su autodeterminación informativa en sí.

Fundamentamos esta posición dado que tanto el género derecho a la intimidad y a la autodeterminación informativa, como su especie, el derecho a la protección de los datos de carácter personal, son ambos derechos personalísimos y por ello irrenunciables. Coincidimos con la doctrina mayoritaria sobre el derecho a la intimidad y, *mutatis mutandi*, postulamos la necesidad de descartar toda interpretación que sobre el contenido y la tutela o protección civil del derecho a la protección de datos personales acepte algún condicionamiento o dependencia en función de los propios actos del pasado, de los usos y costumbres sociales.

La tesis contraria nos llevaría a afirmar que aquellas personas que tienen una honorabilidad debilitada porque no mantuvieron en su vida una actitud de discreción o cautela al proporcionar sus datos personales a terceros carecen de intimidad y derecho a su autodeterminación informativa.

Tal conclusión, como ya lo expresamos, es contraria al principio de irrenunciabilidad que caracteriza a estos derechos. Pero mucho más se evidencia su injusticia en materia de datos personales, puesto que es pública y notoria la forma en que la evolución tecnológica, en interacción con el mundo globalizado, ha penetrado en la sociedad y en la vida diaria de las personas. Esta injerencia en la intimidad de las personas ha alcanzado por igual a las personas públicas, o expuestas a la opinión pública, como a aquellas que no lo están. En la actualidad los datos de todo tipo de personas son absorbidos en forma compulsiva y voraz por los distintos sistemas de obtención de información para el comercio, la seguridad, la banca o las aseguradoras. Además, la gestión de simples trámites domésticos como el tributo de impuestos, la incorporación a los sistemas de salud, de educación, de previsión social y tantos más exige la incorporación de datos personales a distintos sistemas informáticos de bases de datos. Internet sabe sobre nosotros mucho más de lo que creemos, dado que muchas veces sin darnos cuenta vamos dejando nuestros datos personales, nuestros gustos, lo que hacemos o dejamos de hacer en la *web* o en las redes de datos. Por eso, cada vez más empresas se dedican a procesar el comportamiento que tenemos en las redes de información; la procesan y la venden principalmente al mundo de los negocios, del *marketing* y de la publicidad[48].

Pertenecemos a una civilización que constantemente evoluciona tecnológicamente en el tratamiento y acumulación de la información. La mayoría de las personas desconocen los efectos y peligros que les acechan al proporcionar sus datos personales en forma inocente. De alguna manera, propiciamos sin saberlo la vulneración de nuestro más sensible derecho a la intimidad y a la autodeterminación

[48] La Gaceta, (diario de la Provincia de Tucumán, Argentina). "Venden todo lo que la web sabe de nosotros", edición en papel del día 25 de Agosto de 2012.
Fci:http://www.lagaceta.com.ar/nota/507515/economia/red-no-gratis-vos-pagas-tus-datos.html (último ingreso: 25/08/2012).

informativa. La educación y esencialmente las escuelas se encuentran en el peldaño anterior a lo que ocurre en la sociedad, y aún más, los diseños curriculares están profundamente desactualizados con respecto a los cambios que genera la tecnología. La escuela, no cumple la función de preparar al individuo para su protección en esta materia.

Para evitar caer en posturas extremas, pensamos que deben ser ponderadas las circunstancias concurrentes en cada caso, con la sola intención de evitar que las personas puedan quedar convertidas en presas de su pasado o, peor aún, en presas de un consentimiento inocente y desinformado, otorgado por desconocimiento e imprevisión al proporcionar sus datos personales a terceros, sean particulares o administraciones públicas, máxime cuando en no pocas ocasiones implicaría otorgarles responsabilidad por las consecuencias de una decisión tomada sin posibilidad de decidir, es decir, con escasa o nula libertad.

2.2.5.- Usos sociales y conducta del sujeto

Cierto es que en la configuración del derecho a la protección de los datos personales, además del componente individual, que viene representado por la propia conducta, juegan también los usos y la costumbre como un componente de significación social. Sin duda, este componente hace su aporte al configurar el bien jurídico protegido con respecto a la generalidad de las personas, independientemente de la posición socioeconómica o cultural que individualmente ocupe cada una de ellas.

Aun así, la remisión a los usos y costumbres no debe conllevar un trato jurídicamente discriminatorio; por el contrario, debe contribuir a la delimitación de los supuestos, sean cuales sean las personas implicadas, para precisar de forma más justa e igualitaria lo que debe ser tolerado por los individuos en materia de procesamiento, cesión, cruce, transmisión y propagación de sus datos personales. La incidencia negativa de los usos y costumbres, junto al posible riesgo de

discriminación que su operatividad encierra, ha sido, verdaderamente, una cuestión que ha preocupado a la doctrina española.

La alusión a los usos puede en algún momento resultar discriminatoria en la valoración del honor o la intimidad de las personas en detrimento de la justicia. En este sentido, la efectividad de la prohibición de discriminación o del principio de igualdad puede verse comprometida por la subordinación del derecho a unas normas mutables y cambiantes como son los usos sociales[49].

De aceptarse la validez de los usos sociales tanto en materia de intimidad como de derecho a la autodeterminación informativa, la protección de los datos de las personas quedaría condicionada por el ambiente en el que se desenvuelve o por los criterios conforme a los cuales cada uno se rige en sus relaciones con los demás. La intimidad es un componente de la personalidad, necesario para su desarrollo integral, y por ello no puede ser tratada como un privilegio o un patrimonio exclusivo, reservados sólo a la nobleza, a las clases acomodadas o a las personas refinadas o cultas, sino que corresponde a todos como un derecho individual, de alcance universal e irrenunciable de la persona.

Tanto el derecho a la protección de los datos de carácter personal, como los derechos a la intimidad, a la autodeterminación informativa y al honor se enfrentan con el peligro de la relatividad con que se aplique el criterio de los usos sociales para considerar adecuada una mayor o menor protección a una persona determinada.

El problema que se presenta es que los usos sociales suelen considerar que unas personas, por las circunstancias particulares vitales que las afectan, gozarán, en la práctica, de mayor protección que otras, y con ello se produce una reducción del ámbito de este derecho fundamental respecto de estas últimas, como consecuencia de la interpretación dada por los usos sociales y de los comportamientos individuales.

[49] Cabezuelo Arenas, A. (1998). Op. cit., p. 22.

Sin embargo, es necesario alertar que siguiendo esas ideas nos enfrentamos al peligro de hacer menguar y disminuir la propia intimidad y la autodeterminación informativa de una persona[50] que no supo o no quiso reaccionar a tiempo frente a las intromisiones dirigidas contra su persona a partir de la acumulación, procesamiento y cesión de sus datos personales en el pasado. La cuestión adquiere mayor gravedad, dado que el deficiente conocimiento informático o la escaza toma de conciencia sobre los peligros que puede ocasionar el uso desprevenido de las redes sociales o la entrega de datos en sitios de Internet, dejaría a algunas personas con un derecho a su autodeterminación informativa disminuido o debilitado si seguimos el criterio de los usos y costumbres.

El menoscabo o depreciación de la intimidad y de la autodeterminación informativa personal es el telón de fondo del escenario óptimo para generar un ambiente de permisión para la vulneración de los derechos fundamentales en general, que jurídicamente se transformaría en un importante obstáculo para el eficiente progreso de las acciones judiciales de amparo y defensa contra aquellos arbitrarios actos ilícitos que vulneren la autodeterminación informativa de una persona, con el único fundamento de que aquellos sucesos antes fueron tolerados por el mismo sujeto afectado.

Subordinar el contenido y la efectiva defensa del derecho a la autodeterminación informativa al comportamiento del potencial afectado implicaría, aceptar en la práctica la renuncia de un derecho que en la teoría, en la literalidad de la ley o, más aún, en la doctrina aceptada internacionalmente en forma pacífica sobre los derechos personalísimos, se presenta naturalmente irrenunciable.

En otras palabras, en la práctica esta propiedad sobre los derechos a la intimidad, a la autodeterminación informativa y a la protección de los datos personales, es un derecho humano y personalísimo por naturaleza, que

[50] En ciertos casos esto sucede por ignorancia, por desconocimiento o incluso por una falta de preocupación, fomento o incumplimiento del Estado en realizar acciones positivas para formación y toma de conciencia de las personas en la protección de su derecho a la protección de datos y autodeterminación informativa.

paradójicamente quedaría disminuido a una expresión de anhelos sin eficacia jurídica, si subordinamos su defensa a la trayectoria, a los actos y a los usos que la persona vulnerada en su intimidad hubiera realizado en el pasado con sus datos personales.

Ciertamente, el propio comportamiento de proporcionar descuidadamente datos personales a terceros puede crear expectativas y hacer nacer creencias o presunciones en aquellos que acumulan y procesan datos personales ajenos de una continuidad o persistencia futura en seguir autorizando a procesar sus datos personales sin un renovado consentimiento del titular del dato.

Por el contrario, la esencia de los derechos personalísimos puede desvanecer tales esperanzas, puesto que su naturaleza jurídica ampara y protege a las personas en su derecho a cambiar su actitud, a pesar de sus actos del pasado. En estos casos, el ordenamiento jurídico debe tutelar a aquellos que soliciten su protección y debe respetar la decisión del sujeto afectado, basada en su derecho a la libertad y al libre desarrollo de su propia personalidad, aun cuando antes, en el pasado, no hubiera protegido su información personal.

2.2.6.- Derecho al olvido

Sucede que aquí también aparece un derecho muy novedoso, derivado de la doctrina de la autodeterminación informativa y del derecho amplio a la protección de los datos personales, al cual podemos denominar "derecho al olvido", que en términos vulgares Cabezuelo Arenas[51] lo expresa como una especie de "borrón y cuenta nueva" con lo que hasta ese momento había caracterizado la existencia de su persona. En este sentido, encontramos que el derecho al perdón o al olvido y la necesidad de los demás, de estar informados, confluyen en una tensión imposible de disolver[52].

[51] Cabezuelo Arenas, A. (1998). Op. cit., p. 24.
[52] Palazzi, P. La Protección de los Datos Personales en Argentina. Ed. Errepar. Buenos Aires, 2004, p. 171.

Por eso es necesario definir, por ejemplo, el papel que deben jugar las empresas de informes crediticios en nuestra sociedad determinada, ya que este tipo de organizaciones parecen ser un mal necesario, para el funcionamiento del comercio y la economía, porque por un lado, rápidamente informan a las instituciones más vulnerables con quién están negociando; pero, por otra parte, su informe puede ser ambiguo, errado o impreciso, con la consecuente estigmatización del titular del dato mal informado, a veces sobre eventos pasados, que deberían estar olvidados y ausentes de todo procesamiento de datos personales.

La intersección de necesidad y mal causado, requieren de una férrea intervención estatal, que sea firme pero criteriosa para minimizar los abusos de las bases de datos personales y mantener su utilidad. Este es el punto de partida que pensamos debe inspirar a toda la legislación que se dicte sobre este tema y desde el cual fundamentar la justificación de la existencia de autoridades de control independientes y autónomas en materia de protección de datos personales[53].

El derecho al olvido, con los plazos que el legislador determine, sin perjuicio del derecho de la persona a su identidad e historia o del interés público determinados temas, debe ser parte de los desarrollos políticos y regulatorios en materia de la protección de datos personales pensados para nuestro siglo XXI. En tal sentido, pensamos que debe diferenciarse la información recopilada en materia de sanciones a los individuos, que sí debe ser borrada y olvidada al cumplirse los plazos establecidos por la ley, de aquella información relacionada con conceptos sociales de identidad, historia e interés público, la cual por su naturaleza puede, en determinados casos, mantenerse visible en forma permanentemente [54].

---

[53] Fernández Delpech. A. (2008).*Protección de Datos Personales – Derecho al olvido* (en línea), Universidad del Salvador.
Fci: http://www.hfernandezdelpech.com.ar/Trabajo%20Derecho%20al %20Olvido.pdf
(último ingreso: 02 de diciembre de 2009).

[54] Iriarte Ahon, E. (Coordinador de Edición). Informe de Análisis y Propuestas en Materia de Acceso a la Información y Privacidad en América Latina. (Documento desarrollado dentro del Proyecto Monitor de Privacidad y Acceso a la Información en América Latina). Editado por UNESCO. Lima, 2007, p. 16.

Sobre esta categoría especial de datos personales, pensamos que no debe ser negada la protección o requerimiento de autodeterminación informativa, incluso ante la presencia de un ejercicio de exposición de datos personales descuidado, excesivo o irresponsable ante la solicitud de datos en formularios papel, bases de datos, sitios web de internet, redes sociales, etc.

Nos referimos a aquellas personas que habiendo hecho en el pasado voluntarias concesiones de datos personales sobre su propia vida privada, al proporcionar conscientemente información personal en busca de beneficios en determinados ámbitos[55] y pretendan luego ejercer su derecho al olvido o cancelación de esos datos. Es importante resaltar esta idea, dado que la doctrina clásica del derecho a la intimidad sobre la vida social de las personas, sostiene todo lo contrario. Se observa en este tema como las TIC desafían a una constante evolución a la doctrina clásica del derecho.

Pensemos en quienes utilizan las bases de datos de carácter personal para construirse un perfil virtual o informático determinado, aun a costa de ser luego objeto de la intromisión ajena en su vida. A pesar su descuido, o la valoración moral que hagamos de esta conducta de los cibernautas, consideramos que su derecho a autodeterminarse informativamente en el futuro, solicitando el derecho al olvido o la cancelación de ese perfil informático, es legalmente válida por la naturaleza del derecho que se encuentra en debate.

Insistimos en que por la naturaleza jurídica de estos derechos, encuadrados como derechos personalísimos y por lo tanto irrenunciables, los cambios de actitud informativa del sujeto sobre sí mismo, deben ser siempre respetados.

La construcción de una fuerte doctrina sobre la protección de los derechos a la intimidad, y en particular a la autodeterminación informativa y a la protección de los datos de carácter personal, debe ser el límite a la proliferación de bases de datos

[55] Por ejemplo en sitios o páginas web de Internet que relacionan personas con distintos fines.

de carácter personal que no cuenten con el consentimiento del titular del dato o que no respeten su voluntad autodeterminativa.

La mayoría de los responsables de estas bases de datos de carácter personal actúan como si tuvieran el derecho absoluto a incursionar en forma ilimitada e indefinida en aquella zona de reserva de los individuos ya descripta, y toman como justificación la precedente permisividad de los afectados para un prolongado o incluso eterno uso de tales datos personales en el tiempo futuro.

La protección del derecho a autodeterminación informativa no debe limitarse a criterios subjetivos, y en principio y salvo el consentimiento expreso e informado, sean cuales sean los actos realizados por las personas con sus datos personales, a todos debe proteger la ley por igual.

La doctrina clásica sobre el derecho a la intimidad opina todo lo contrario a lo sostenido por esta tesis en este punto. La mayoría de los autores piensan que las actitudes individuales repercuten en la posibilidad de alegar la existencia de un derecho o, por el contrario, hacen inviable e insostenible una futura reclamación a todas luces incompatible con lo que se ha dado a entender o con lo que se ha propiciado.

Ana Cabezuelo Arenas expresa que el papel de los propios actos, en general, debe ser interpretado en forma restrictiva dentro del derecho a la intimidad[56]. Esta interpretación, continúa, nos permite superar teorías que se basan en otorgar al comportamiento de cada persona una importancia desmesurada en la configuración del derecho en cada caso particular. Evitaríamos con ella que pudiera verse en peligro, -como ya adelantamos- la irrenunciabilidad de los derechos a la autodeterminación informativa y a la protección de los datos de carácter personal, pues, lejos de concluirse que quien fue cediendo ocasionalmente en materias íntimas o privadas, disfrute tras ello de un menor ámbito de protección que otras personas. En caso contrario, se aceptaría que la disposición sobre la intimidad

[56] Cabezuelo Arenas, A. (1998). Op. cit., p. 19.

estuviera llamada a operar únicamente en el ámbito en el que se efectuó. Imaginemos que se decidiese en una ocasión concreta proporcionar datos personales que atañen a la vida privada, relativos, por ejemplo, a las propias creencias religiosas. Por frecuentes que sean las cesiones de datos que el titular realice, no quiere ello decir que disfrute de una intimidad menor que la que cabe predicar respecto de a otra persona. Si esto se defendiera, la asiduidad con que alguien entregue datos sobre materias o aspectos privados, aunque fuesen siempre los mismos, propiciarían que el juzgador los justifique en la desesperación –o incluso frivolidad– en la significación que estos derechos tienen para su titular.

Naturalmente, no se podría alegar violación de la intimidad cuando, en una base de datos determinada, por ejemplo en una red social de Internet, se autorice a publicar en su perfil personal su calidad de persona atea, puesto que el mismo habrá fomentado esos comentarios, pero nada le impide defender otros aspectos de su intimidad sobre los que no ha efectuado concesiones. O incluso si cambia su condición de ateo a creyente, exigir ese cambio en el perfil. O más aún si esa persona continúa siendo atea, pero no desea la exposición de ese dato, tiene el pleno derecho a exigir que no sea expuesto o incluso a que sea borrado y cancelado de la base de datos.

En la práctica encontramos que, con respecto al derecho a la intimidad, la jurisprudencia suele considerar la conducta anterior como un todo, y que, a la hora de estimar si se produjo o no una intromisión en su zona de reserva, no se debe tratar de la misma forma a personajes discretos que a los que han dedicado su vida a mostrar y contar sus intimidades (incluso cuando aquellos datos que expusieron no guarden conexión alguna con los hechos que fundamentan su demanda: pueden haber expuesto datos sobre su vida sexual, pero no tienen, por esta causa, por qué soportar que trascienda su mala situación económica o su credo religioso).

Esta posición clásica de la jurisprudencia con respecto al derecho a la intimidad, debe variar al momento de juzgar casos de derecho a la autodeterminación informativa o protección de los datos personales, dadas las

diferencias de naturaleza entre uno y otro derecho, aun cuando el derecho a la intimidad pueda ser entendido como el género del cual se desprende el derecho a la autodeterminación informativa como especie del mismo.

2.3.- Intimidad y autodeterminación informativa

La autodeterminación informativa integra el aspecto o concepto subjetivo del derecho a la intimidad[57]. Mientras el concepto objetivo de derecho a la intimidad atiende en esencia a la etimología del concepto como una "zona espiritual reservada o íntima de una persona o de un grupo, especialmente de una familia"[58], el concepto subjetivo fue concebido por primera vez en la Sentencia del Tribunal Constitucional Alemán de 1983[59] relativa a Ley del Censo de Población.

El Tribunal Constitucional alemán expresó en la sentencia mencionada, que la autodeterminación informativa encuentra fundamento normativo en el artículo 2 de la Ley Fundamental de la República Federal Alemana (Bonn, 1949)[60], que establece la facultad del individuo derivada de la idea de autodeterminación, de decidir básicamente por sí mismo, cuándo y dentro de qué límites procede a revelar situaciones referentes a la propia vida[61].

Observamos que el TCA fundamentó su fallo en una concepción subjetiva del derecho a la intimidad, que se identifica con el ámbito de plena disponibilidad por parte del individuo, que en ejercicio de su libertad determina lo que debe o no

---

[57] Rebollo Delgado, L. y Serrano Pérez, M. (2008), (2º Edición). *Introducción a la Protección de los datos*. Madrid: Ed. Dykynson; p. 36.

[58] Intimidad: Segunda acepción: "Zona espiritual reservada o íntima de una persona o de un grupo, especialmente de una familia". Diccionario de la Real Academia Española de la Lengua. Op. cit., p. 1183.

[59] Fuente consultada en Internet: http://www.informatica-juridica.com/jurisprudencia/alemania.asp (último ingreso el 5/8/2012). El sitio oficial del Tribunal Constitucional Alemán se encuentra en la siguiente dirección web en Internet: http://www.bundesverfassungsgericht.de/

[60] Ley Fundamental de la República Federal Alemana (Bonn, 1949). Más conocida con Ley Fundamental de Bonn. Fci.:
http://www.buenos-aires.diplo.de/contentblob/2227504/Daten/375140/Grundgesetz_Download.pdf

[61] Ley Fundamental de la República Federal Alemana (Bonn, 1949). Art. 2. Libertad de acción y de la persona. 1) Toda persona tiene derecho al libre desarrollo de su personalidad siempre que no viole los derechos de otro ni atente contra el orden constitucional o la ley moral.

quedar fuera del conocimiento de los demás. Esta sentencia expresa que estar en libertad es la capacidad de una persona para decidir por sí misma. En otras palabras: estar en libertad es el poder que tiene cada persona de autodeterminarse informativamente.

La jurisprudencia española ha recurrido a este concepto en diferentes sentencias, al indicar que el derecho a la intimidad es una facultad para excluir a los demás o exigir la abstención de sus injerencias. Acepta un ámbito propio de la vida privada personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo que hayan sido consentidas por el interesado.

Mientras el aspecto objetivo del derecho a la intimidad se identifica con la protección de un ámbito concreto que el individuo tiene derecho a defender; con fundamento en la dignidad que tiene como persona y que debe ser respetada por los demás, el concepto subjetivo se fundamenta en la libertad que tiene toda persona y que es la base de todos sus derechos.

El derecho a la autodeterminación informativa se presenta como una extensión de la idea de derecho a la intimidad, dado que va más allá de la simple defensa de un ámbito de reserva y otorga a toda persona el derecho a intervenir en aquello que está fuera de ese ámbito interior y que aun estando fuera de él, lo afecta.

Entendido de esta forma, el concepto de autodeterminación informativa implica una actitud activa por parte del individuo: la acción de ejercer el derecho a controlar lo que de él se conoce. Es el derecho a controlar los datos que son relativos a la propia persona, y para garantizarlo, el ordenamiento jurídico debe establecer un mecanismo necesario para hacerlo efectivo.

De esta forma intimidad y autodeterminación informativa son términos que están conectados entre sí. Por lo tanto, el ejercicio del derecho a la protección de los datos de carácter personal implica a su vez el ejercicio del derecho a la intimidad y a la autodeterminación informativa.

La autodeterminación informativa es el fruto de una reflexión doctrinal combinada con las elaboraciones jurisprudenciales de diferentes tribunales, de diferentes países, sobre el control por parte del sujeto afectado, de las informaciones que se refieren a su persona o a su familia.

La doctrina del derecho a la autodeterminación informativa se construyó desde la noción de intimidad (en el idioma castellano) o sus términos equivalentes, *privacy*, *riservatezza* o *vie privée,* en otras lenguas. Su objetivo se encamina, fundamentalmente a dotar a toda persona, de una tutela jurídica concreta, frente al peligro que supone la informatización de sus datos personales.

Los sistemas jurídicos del mundo occidental, en general, han desarrollado el derecho de autodeterminación informativa a partir de un concepto amplio de intimidad, centrado especialmente en la voluntad de cada individuo afectado. De esta manera, el derecho a la intimidad vedaría, en principio, toda intromisión en aquellas esferas de la vida que el titular quiere reservar para sí.

Si el derecho a la intimidad incluye la facultad de vedar el acopio y utilización de información personal, así como el control sobre esta última cuando se consienta o se realice por mandato legal, entonces podemos también incluir dentro de su alcance a la tutela de los datos personales que se procesan por medio de sistemas informáticos.

El aspecto de la intimidad relacionado con el control de la información personal plantea perfiles absolutamente nuevos con la irrupción de las nuevas tecnologías y, especialmente, con el uso generalizado de la informática; aun así, es evidente la cercanía o coincidencia entre el derecho a la intimidad, el derecho a la autodeterminación informativa y la protección de los datos de carácter personal.

De todas formas, puede ocurrir que los problemas específicos que plantea la informática hagan conveniente organizar la defensa jurídica del ciudadano en lo que toca a sus datos personales desde una posición de independencia sistemática

respecto de los otros perfiles de la intimidad. Razones dogmáticas, en un caso, y prácticas en el otro, pueden aconsejar la diferenciación.

Por este motivo entendemos que los estudios que han considerado los problemas relativos al derecho a la intimidad se han centrado en su protección civil o en la tutela penal que tradicionalmente ha pretendido asegurar la inviolabilidad del domicilio o el secreto de las comunicaciones, en cambio, la libertad informática y el derecho a la autodeterminación informativa se concretan en la garantía de acceso y control de la información que ejercen las personas a quienes les conciernen estos derechos.

En la doctrina, el derecho a la autodeterminación informativa es concebido como una categoría más estricta, como un aspecto del libre desarrollo de la personalidad o como una faceta de la intimidad, o facultad que tienen las personas de conocer y acceder a las informaciones que a ellas se refieren, archivadas en bancos o bases de datos[62]. Una vez que la persona concreta el acceso a esa información, el ejercicio del derecho a la autodeterminación informativa incluye también la facultad de controlar su calidad; es decir, la posibilidad de corregir o cancelar los datos indebidamente procesados y autorizar o no su cesión o transferencia. El derecho a la autodeterminación informativa fue incluido en muchas constituciones como una garantía constitucional o proceso de amparo y tutela especial, sobre los datos personales, es también conocido como *habeas data*[63]**.** La protección jurídica de los datos de carácter personal por medio de la acción constitucional de *habeas data* es el camino que en general ha seguido América, con la excepción de EEUU y Canadá. La mayoría de los países que siguieron este camino en América, ya desarrollaron la norma constitucional de *habeas data* con legislaciones y reglamentos de protección de datos personales.

---

[62] Denniger, E. *El derecho a la autodeterminación informativa*. Publicado en: *Problemas actuales de la documentación informática jurídica*. Madrid, Editorial Tecnos, año 1987, p. 274.
Murillo de la Cueva, L. *El derecho a la autodeterminación informativa*. Editoriales Tecnos. Madrid, 1990, p. 147.

[63] Ver capítulo 1, punto 5 de esta tesis.

La intimidad tutelada por el derecho a la autodeterminación informativa, tiene una proyección política y colectiva. El fenómeno informático en relación con la intimidad supera los viejos esquemas que convertían en compartimientos estancos lo individual y lo social, lo personal y lo colectivo, lo público y lo privado. Desde esta perspectiva, el derecho a la intimidad se encuentra en relación con otros derechos y libertades. Por ello, el mal uso que se haga de las nuevas tecnologías de la información y de las comunicaciones afecta también a otros valores, entre los que se encuentran algunos tan importantes como la libertad o la igualdad. En otras palabras, las TIC no suponen solamente la posibilidad de un conflicto con algún derecho o libertad concreta, sino que además amenazan el carácter pluralista y democrático de nuestra sociedad, situación magistralmente descripta por el novelista George Orwell en su libro *1984*[64].

Vemos que frente a la creciente voracidad de las administraciones (del sector público y también del sector privado) sobre el acceso a las parcelas más reservadas de los ciudadanos, justificada, en cierto modo, por la necesidad de logra un funcionamiento eficaz del Estado o de la institución de que se trate, existe en los ordenamientos jurídicos más evolucionados en el respeto por los derechos humanos, una tendencia cada vez más firme a proteger las bases de datos personales por el peligro de invasión que afecta a la persona y a su autodeterminación informativa.

La intimidad se puede preservar mediante la autodeterminación informativa: esa es la importancia de este derecho que tienen las personas a decidir por sí mismas cuándo y dentro de qué límites procede revelar datos referentes a su propia vida.

Este término aparece en la jurisprudencia, por primera vez, en la sentencia del Tribunal Constitucional Alemán del 15 de diciembre de 1983, relativa a la Ley del Censo de la República Federal Alemana.

El pronunciamiento jurisprudencial es coincidente con una preocupación humana, surgida en la segunda mitad del siglo XX, sobre los riesgos generados por

[64] Orwell, G. (2010), (1ª ed.1966). Op. cit.

las TIC a la noción tradicional de intimidad culturalmente concebida. La protección jurídica a la intimidad existente hasta esos tiempos era insuficiente para proteger a las personas frente al peligro de invasión que representaban las TIC, y era necesario una nueva noción o concepto de intimidad: la intimidad informativa.

Esta nueva expresión, buscaba dar la protección jurídica a las personas frente a la captación y utilización no autorizada de información personal. Diversos autores lo expresan en sus obras a partir de la segunda mitad del siglo XX; entre ellos Alan Westin en 1967 (*Privacy and Freedom*), Arthur Miller en 1971 (*Personal privacy in the compute rage: The challenge of new technology in a Information oriented society*), Guido Alpa (*Privacy e estatuto dell´informazione*), o Richard Hixson (*Privacy in a public society*[65]).

A partir de esta distinción, entre intimidad e intimidad informática, se edificó un sistema de protección de datos en Gran Bretaña. Durante el periodo de trabajos preparatorios para la ley británica aparece el *Informe Younger* (*The Younger Committee Report on Privacy*)[66], documento publicado en 1972 en el que se distinguen dos facetas de la intimidad:

a) La intimidad física. Supone la libertad frente a toda intromisión sobre uno mismo, también en su casa, en su vida familia o en sus relaciones personales.

b) La intimidad informativa. Supone el derecho a determinar personalmente cómo y en qué medida se puede comunicar a otros alguna información sobre uno mismo.

[65] Hixon, R. *Privacy in a Public Society. Human Rights in Conflict.* Ed. Oxford University Press. EEUU, 1987.

[66] Sobre el Informe del Comité sobre la Intimidad (*The Younger Committee Report on Privacy*), ver: Dworkin, R. *The Modern Law Review* Vol. 36, No. 4 (Jul., 1973), pp. 399-406. Published by: Wiley Article Stable. Fci.: URL: http://www.jstor.org/stable/1093890http://www.jstor.org/discover/10.2307/1093890?uid=3737512&uid=2129&uid=2&uid=70&uid=4&sid=21101169382977 (ultimo ingreso el 25/08/2012).

En base a estos antecedentes, diez años más tarde, el Tribunal Constitucional alemán perfila con mayor precisión un concepto de intimidad informativa al hablar de autodeterminación informativa. Por este motivo, diferentes autores expresan que el derecho a la autodeterminación informativa no fue una creación del Tribunal Constitucional alemán. Entienden que la célebre sentencia del TCA, del 15 de diciembre de 1983, relativa a la Ley del Censo de la República Federal Alemana sólo vino a completar una línea jurisprudencial especial de los tribunales alemanes con respecto al derecho general a la personalidad y a su autodeterminación.

La sentencia del TCA manifiesta la necesidad de establecer un equilibrio entre la autodeterminación informativa (reflejo de las libertades individuales y del derecho de la intimidad) y el derecho a la información en su doble vertiente de recepción y comunicación de información.

En la sentencia queda claramente expresado que la normativa debe permitir la existencia y el funcionamiento de los bancos de datos, pero el progreso y la gestión eficiente de la administración pública o del sector privado, no deben avanzar a costa de un recorte de las libertades individuales de la persona. Declara inconstitucionales algunos artículos de la Ley del Censo de la República Federal Alemana, por afectar los derechos a la intimidad y a la vida privada de las personas. Expresa que las personas tienen derecho la autodeterminación informativa, es decir, que poseen un derecho de libre decisión sobre sus datos personales, sobre los cuales pueden decidir qué es lo que permiten que otros sepan sobre ellos.

De esta forma se configura, a partir del derecho general de protección de la persona (artículos 1º y 2º de la Ley Fundamental de Bonn)[67], la idea de

[67] *Ley Fundamental de la República Federal Alemana*. Traducción publicada por el Departamento de Prensa e Información del Gobierno Federal Alemán. Preparada por la Sección de Interpretación de Idiomas del Ministerio de Relaciones Exteriores de la República Federal de Alemania. Esse Werden, 1971. Artículo 1. 1. La dignidad del hombre es intangible. Respetarla y protegerla es obligación de todo poder público.2. El pueblo alemán se identifica, por lo tanto, con los inviolables e inalienables derechos del hombre como fundamento de toda comunidad humana, de la paz y de la justicia en el mundo. 3. Los siguientes derechos fundamentales vinculan a los poderes legislativo, ejecutivo y judicial a título de derecho directamente aplicable. Artículo 2. 1. Todos tienen derecho al libre desenvolvimiento de su personalidad, siempre que no vulneren los derechos de otro ni

autodeterminación para decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida.

El fallo señala que las limitaciones al derecho a la autodeterminación informativa sólo pueden fundamentarse en un interés general superior cimentado por la Constitución. En su texto, aconseja que la normativa de regulación de los bancos de datos adopte precauciones procesales que respeten el principio de proporcionalidad y sean aptas para contrarrestar el peligro de vulneración del derecho a la protección de la personalidad.

Declara lícita la recolección de los datos del censo referidos a nombre, apellidos, dirección, estado civil, nacionalidad, utilización de la vivienda, fuente de los medios principales de subsistencia, datos académicos y profesionales, rama de actividad. Pero, a su vez, declara ilícitos algunos artículos de la ley, entre otros, los referidos al cruzamiento de datos para ser utilizados contra las personas obligadas a suministrar la información. Busca evitar que los datos de carácter personal, recogidos y empleados con fines demográficos y científicos, sean usados con finalidades distintas a aquellas para la cual fueron recabados.

El Tribunal Constitucional alemán logró con este pronunciamiento jurisprudencial que el derecho a la intimidad deje de ser sólo un status negativo para convertirse en un status positivo y activo de la persona. A partir de este fallo, el derecho a la intimidad dejó de ser una actitud pasiva de simple defensa de nuestra intimidad, delimitadora de un ámbito de no interferencia, para transformarse en una postura activa que tienda a ejercer el control sobre la información personal existente en los diferentes bancos de datos. El fallo en análisis impulsó la aprobación de nuevos y diversos instrumentos internacionales que reconocieron el derecho a la intimidad informativa, o derecho a la autodeterminación informativa, en todo el mundo.

---

atenten al orden constitucional o a la ley moral.2. Todos tienen derecho a la vida y a la integridad física. La libertad de la persona es inviolable. Estos derechos solo podrán ser coartados en virtud de una ley.

Sin lugar a dudas esta sentencia tiene un gran valor histórico ya que viene a marcar un hito en la defensa de los derechos de la persona a preservar su vida privada. El recurso contra la Ley del Censo, sobre el cual trata el pronunciamiento del TCA, fue presentado por simpatizantes del grupo político conocido en Alemania como "los verdes", quienes obtuvieron una resolución cautelar del Tribunal Constitucional el 13 de abril de 1983, por la que se suspendió la entrada en vigor de la Ley del Censo y posteriormente la decisión definitiva sobre el fondo del recurso.

El Tribunal Constitucional germano señala en el fallo que la proliferación de centros de datos ha permitido, gracias a los avances tecnológicos, producir "una imagen total y pormenorizada de la persona respectiva -un perfil de la personalidad-, incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en "hombre de cristal". El TCA fue rotundo al establecer que la persona posee un derecho de libre decisión y libre disposición sobre sus datos personales y que puede decidir qué es lo que otros pueden saber sobre ella.

La doctrina de la autodeterminación informativa llega casi un siglo después de la publicación del ensayo de Warren y Brandéis, *The Right to Privacy*, sobre el derecho a la intimidad (*privacy*). Cierto es el derecho a la intimidad (o *privacy* en el derecho anglosajón) evoluciona a partir del ya mencionado artículo de los juristas Warren y Brandéis. Pero en esta doctrina, el derecho a la intimidad es entendido como un derecho que puede necesitar ejercer tan sólo una clase acomodada o determinadas personas expuestas a la alta exhibición pública.

En cambio, la doctrina del TCA sobre el derecho a la autodeterminación informativa se ubica en el tiempo del tránsito entre la segunda y la tercera generación de leyes de protección de datos personales. A partir del contenido de este fallo va a evolucionar a pasos agigantados el derecho a la protección de los datos de carácter personal. Sin embargo, es válido insistir en que el pronunciamiento jurisprudencial del TCA es coincidente con una preocupación humana, surgida ya, a partir de la segunda mitad del siglo XX, sobre los riesgos generados por las TIC a la noción tradicional de intimidad culturalmente concebida.

En 1983 existían diversos antecedentes para fundar el derecho a la autodeterminación informativa y es interesante destacar que casi dos años antes, el 28 de enero de 1981, el Consejo de Europa[68] había aprobado el Convenio 108 para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal[69].

La doctrina de los juristas es pacífica al aceptar que el término autodeterminación informativa fue usado por primera vez en esta sentencia del Tribunal Constitucional alemán. Pero también es cierto que la línea jurisprudencial seguida por los tribunales alemanes relativa al derecho general a la personalidad fue respetada y ampliada por el TCA para fundamentar la necesidad de garantizar un equilibrio entre los derechos a la intimidad y a la información.

2.4.- Intimidad y protección de los datos

En 1960, un poco más de veinte años antes del pronunciamiento del TCA sobre el derecho a la autodeterminación informativa, la humanidad había recibido una primera una alerta, un aviso que le permitió comenzar a tomar conciencia del peligro que genera a la intimidad personal el procesamiento automatizado de datos personales. Sucedió durante la década de 1960 cuando el gobierno francés intentó implementar un proyecto llamado SAFARI (*Système Automatise pour les Fichiers Administratifs et le Répertoire des Individus*).

Con la implementación de este sistema, el gobierno galo buscaba implantar un plan de atribución, para cada ciudadano, de un número de identificación común para todas las relaciones con los diversos departamentos administrativos del Estado.

La opinión pública francesa polemizó con el proyecto del gobierno, y se generó una gran crisis política. Seguramente el motivo de la polémica haya sido el ingenioso nombre de SAFARI, que caricaturizaba a este sistema como una

[68] Fci: http://www.coe.int/ . Op. Cit., Concejo de Europa (último ingreso: 18/11/2010).
[69] Fci: http://www.ifai.org.mx/pdf/ciudadanos/sitios_de_interes/datos_personales/Convenio108.pdf Convenio 108 del Consejo de Europa (último ingreso: 25/8/2012).

novedosa forma gubernamental de cazar a las personas por medio de los sistemas de información del Estado.

Para salvar la crisis política, Valery Giscardd´Estaing, Presidente de la República Francesa encargó al Inspector General de Finanzas Simón Nora y a su subordinado, el Inspector de Finanzas Alain Minc, un informe que llevó por título: *La informatización de la sociedad*[70]. El resultado de la investigación sostiene que la sociedad informatizada es consecuencia necesaria del desarrollo tecnológico, y que su orientación futura depende del equilibrio entre los poderes estatales y del fortalecimiento de la sociedad civil[71]. Los autores del informe anunciaban que la informática iba a cambiar nuestras vidas, y destacaban la necesidad de una política que controle el desarrollo de esta nueva tecnología.

El informe Nora y Minc permitió, entre otros efectos, que los gobiernos europeos tomaran conciencia del peligro que implicaba la informatización de la sociedad para la intimidad de las personas y la necesidad de dictar normas que limitaran el uso de la tecnología en la acumulación de datos personales.

Así surge en Europa una primera generación de leyes de protección de datos personales, que luego evoluciona a remolque de los avances tecnológicos.

La solución normativa dada al problema que la revolución tecnológica ha causado a la humanidad surgió inmediatamente. No hay muchos antecedentes en la historia del derecho positivo sobre una respuesta tan rápida a una incitación o cambio social y tecnológico como el caso de las legislaciones de protección de datos personales. En contraste con las regulaciones jurídicas más tradicionales del derecho privado (Derecho de Sucesiones, Derechos Reales, Obligaciones, Contratos, etc.), las cuales necesitaron el sedimento de largos siglos para organizar sus instituciones, establecer principios y organizar perfiles normativos claros; todo

[70] Nora, S.; Minc, A. La Informatización de la Sociedad. (Trad. Paloma García de Pruneda y Rodrigo Ruza). 1ª edición en Biblioteca Actual. Editorial Fondo de Cultura Económica. Ediciones Nuevo País. (Colección Biblioteca Actual). México, 1987. (1ª edición en francés, 1978; 1ª edición en español, 1980). Título original: *L´informatisation dela société.*

[71] Ibidem, p. 18.

lo contrario ocurrió con la legislación de protección de datos personales que se decantó rápidamente en pocos años por medio de un proceso de convergencia legislativa[72].

En un lapso menor a diez años surgió la primera generación de leyes de protección de datos de carácter personal. Austria, Dinamarca, Noruega y Francia pusieron en vigor en forma casi simultánea sus leyes sobre datos personales.

Esta primera generación de leyes de protección de datos buscó establecer límites a la utilización de la informática, y para ello se concentró en reglamentar el funcionamiento de los bancos de datos existentes en esa época.

Los problemas que exigieron e inspiraron esta pionera generación de leyes eran los más visibles del fenómeno y muchos aspectos sustanciales del problema permanecían ocultos. Por este motivo, estas leyes no diseñaron un sistema de control muy estricto sobre los bancos de datos informáticos, dado que, en esos tiempos, los bancos de datos informáticos eran fácilmente localizables, requerían mucho espacio físico, tenían un gran tamaño, escasa velocidad, complejidad de procesamiento, y no se interconectaban con otros equipos.

La primera ley de protección de datos personales fue promulgada por el parlamento del *Land de Hesse*, en la hoy ya inexistente República Federal Alemana. Fue esta una ley de protección de datos personales de primera generación que sirvió de modelo para las sucesivas iniciativas legales, que no demoraron en ser promulgadas. Dentro de este primer grupo de leyes de primera generación en materia de protección de datos personales podemos mencionar a las regulaciones legislativas de Austria, Dinamarca, Noruega, Francia y Suecia.

La evolución tecnológica perfiló otros órdenes de problemas no contemplados por las leyes de protección de datos vigentes hasta ese momento.

---

[72] *Informática. Leyes de Protección de Datos (II)*. Documentación Informática N° 3. Serie Verde/ Legislación. Presidencia del Gobierno (España). Servicio Central de Publicaciones. Servicio Central de Informática. Ed. Imprenta Nacional del Boletín Oficial del Estado. 1ª ed. Abril de 1983. Madrid, 1983, p. 9.

Estos nuevos problemas junto con la proliferación de bancos de datos informatizados exigió la promulgación de una segunda generación de leyes de protección de datos personales.

También en esos tiempos las telecomunicaciones logran grandes avances que permiten la aparición de nuevos bancos de datos más versátiles, veloces y eficaces en la búsqueda de información Se hizo necesaria un segunda generación de leyes de protección de datos personales que se focalizó en asegurar la calidad de los datos mediante cláusulas específicas de protección de la información con inmediata incidencia sobre la vida privada o sobre el ejercicio de las libertades personales. Estas leyes crearon el derecho de acceso y el derecho a controlar las informaciones por parte de las personas afectadas.

En 1974, en los EEUU entra en vigencia la *Privacy Act,* dos años más tarde se incorpora la protección de la intimidad frente al uso de la informática en la Constitución portuguesa de 1976. En 1978 se aprueba en Francia la ley relativa a la informática, a los ficheros y a las libertades de las personas; ese mismo año, en España, se incorpora el artículo 18 en la Constitución española. El precepto Constitucional del derecho a la intimidad informática llega a la Constitución Española por medio del artículo 18. Estas normas forman parte de la segunda generación de leyes de protección de datos de carácter personal.

Pocos años más tarde llega la Sentencia del Tribunal Constitucional alemán, ya tratada en el punto anterior, la cual, junto a los principios aprobados por el Consejo de Europa[73], en el Convenio 108, va a tener una influencia determinante en la promulgación de nuevas leyes sobre protección de datos personales y con ellas una importante actividad de la doctrina de los autores y de la jurisprudencia, en esta materia.

[73] CE (Consejo de Europa): Convenio 108 para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (Op. cit., fci.), de 28 de enero de 1981. Capítulo II.

Las leyes de protección de datos personales de tercera generación llegan en la década de 1990 con la consigna de regular bancos de datos personales gestionados por sistemas informáticos aún más veloces que aquellos que intentaron controlar las generaciones anteriores, bancos de datos ahora interconectados a redes de alcance mundial, soportados por *hardware* diseñado a partir de la microelectrónica, y por lo tanto más pequeños. Estas nuevas bases de datos son de fácil y rápido traslado, cuentan con una alta capacidad de procesamiento de la información en forma ágil y versátil. Son los tiempos de la evolución de la microelectrónica, la digitalización de la información y la conexión de grandes redes de comunicación con bases de datos personales. Por este motivo surge esta tercera generación de leyes de protección de datos personales, que busca adaptar esta legislación a los nuevos tiempos que y a los desafíos tecnológicos que plantea la década de 1980.

Las grandes computadoras son reemplazadas por pequeñas computadoras personales que se conectan a bancos de datos almacenados en soportes informáticos difíciles de rastrear y encontrar, por su escaso tamaño físico y mucho más difíciles de controlar.

Esta nueva generación de leyes va a intentar armonizar la defensa de los datos personales con las necesidades tecnológicas de la sociedad. Entre las leyes de esta tercera generación podemos mencionar a la *Data Protection Act* del Reino Unido de Gran Bretaña (1984); la LORTAD española LO 5/92, ya derogada y reemplazada por LOPD (Ley Orgánica de Protección de Datos de Carácter Personal 15/99) en diciembre de 1999; el Convenio 108 del Consejo de Europa, promulgado en 1981, y la Directiva Europea 95/46/CE de la Unión Europea, entre otras.

También en década de 1990 el derecho a la protección de los datos personales da sus primeros pasos en América a través de la incorporación de la garantía constitucional conocida como *habeas data*, en casi todas las constituciones de la región.

Observamos que la escasa legislación de protección de datos promulgada en América está pensada para proteger la intimidad de las personas en un mundo dominado por las TIC. Sin embargo, en esas pocas normas americanas, las autoridades de control y aplicación de las leyes de protección de datos personales no están contempladas, y aquellos excepcionales casos en los que fueron previstas, son extremadamente débiles y dependientes del Poder Ejecutivo. En los escasos países donde fueron creadas autoridades de aplicación, ellas carecen de autonomía, de independencia y de recursos presupuestarios propios que les permitan cumplir correctamente sus misiones y fines.

En esta cuestión, la legislación de tutela vigente en Europa no guarda equivalencia con la protección jurídica diseñada en América para proteger a las personas en el control de sus datos personales, dado que los ordenamientos jurídicos europeos se caracterizan por contar con organismos de control independientes.

En muchos Estados americanos el derecho a la protección de datos personales aún no fue incorporado en sus constituciones. En otros, las garantías constitucionales incorporadas en sus cartas magnas son frágiles y su contenido no está desarrollado en una legislación que busque proteger con solidez la información personal. Aquellos ordenamientos jurídicos que ya han promulgado una legislación que desarrolla las garantías constitucionales de protección de datos personales, aún carecen de una autoridad de aplicación independiente que pueda velar por el cumplimiento de la normativa sobre protección de datos personales. En este sentido, planteamos la necesidad de armonizar la legislación sobre protección de datos personales, no solo en América latina, sino en todo el mundo, mediante la formulación de conceptos comunes y universales, como también en las estructuras normativas, en la medida que la legislación local lo permita.

Cierto es que prácticamente todas las legislaciones del mundo protegen el derecho a la intimidad en forma genérica, pero entendemos que para alcanzar una protección eficaz de la intimidad, hoy es necesario que además de una norma constitucional expresa de protección de los datos personales, exista también una ley

que desarrolle el precepto constitucional, determinando un procedimiento concreto con reglas procesales claras que garanticen protección al titular del dato, junto a la existencia de un órgano de aplicación y control apto para velar por el cumplimiento de la ley.

La enunciación de los derechos o garantías constitucionales debe ir acompañada de un debido proceso. Son muchos los derechos y libertades que enumeran las Constituciones, pero no así los mecanismos reales con los cuales aquellos se pueden proteger efectivamente.

Pensamos que no es válido justificar la ausencia de una ley que desarrolle y reglamente la norma constitucional en el escaso uso dado hasta el momento al instituto y en los magros presupuestos nacionales, dado que la pomposa enunciación de derechos sin la correlativa determinación del trámite aplicable concreto, no deja de ser una simple expresión de deseos de protección, que no tutela seriamente los derechos fundamentales de las personas.

Está claro que no es posible dar protección jurídica efectiva a los datos de carácter personal solo mediante declaraciones de derechos que en la práctica carecen de una correlativa aplicación real. Por el contrario, el legislador debe aprobar normas que diseñen con cuidado un órgano de control y aplicación de la ley, que vele por su cumplimiento.

La autoridad u órgano de control y aplicación de la legislación de protección de datos personales, necesita contar con autonomía, con independencia legal y con cierta autarquía financiera. En ella es aconsejable la organización de un registro de bases de datos y un sistema de inspecciones eficaz, que cuente con recursos humanos y técnicos.

Probablemente los magros presupuestos nacionales y las necesidades básicas insatisfechas de la población pueden hacernos pensar que destinar recursos a un órgano de aplicación que controle la protección de los datos personales sería una acción política superficial, que desconoce la cruel realidad que estas naciones viven.

Sin embargo, como ya lo expresamos en el capítulo I, entendemos que la protección de los datos de carácter personal es un derecho humano de tercera generación, un derecho fundamental que requiere una protección especial que garantice la dignidad de las personas y el desarrollo integral de sus personalidades. Es por eso que sostenemos la utilidad y la necesidad de afectar recursos en esta materia para proteger a las personas, que son centro, causa y fin de todo sistema jurídico.

También es necesario contar con una política de difusión del derecho a la protección de los datos de carácter personal, destinada a lograr que las personas tomen conciencia del peligro que acecha a su intimidad en los abundantes procesamientos de datos que caracterizan a la sociedad de la información. Para ello el Estado moderno debe tomar conciencia de esta necesidad y difundir los derechos que tiene cada persona, actuando en forma proactiva por medio de acciones positivas de información y formación ciudadana. Probablemente esta sea la política más eficaz que pueda desarrollar el Estado para tutelar el derecho a la autodeterminación informativa.

Corresponderá al organismo de aplicación y control de la ley de protección de datos personales[74] ejecutar estas campañas de difusión del derecho a la autodeterminación informativa, Al mismo tiempo informa a la ciudadanía sobre su existencia, lugar y forma de realizar toda reclamación en la materia.

La importancia de la creación de un órgano de aplicación y control, autónomo e independiente del Poder Ejecutivo fue claramente expresada por el Grupo de Trabajo Sobre Protección de Datos de la Unión Europea[75] en el "Dictamen 4/2002 sobre el nivel de protección de datos en la República Argentina". El Grupo de Trabajo Sobre Protección de Datos de la Unión Europea observó a la legislación argentina de protección de datos personales y recomendó la creación de

[74] AEPD (España); DNPDPA (Argentina).

[75] El Grupo de Trabajo Sobre Protección de Datos de la Unión Europea fue creado por el artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo independiente de la UE sobre Protección de Datos y Vida Privada. Sus tareas y funciones fueron definidas por el artículo 30 de la Directiva 95/46/CE y por el artículo 14 de la Directiva 97/66/CE.

una autoridad de control y aplicación de la ley, independiente y autónoma del Poder Ejecutivo[76].

La ausencia de leyes y órganos de control en materia de protección de datos personales en América impide alcanzar una adecuada protección del derecho a la intimidad y a la autodeterminación informativa de las personas. Tanto el derecho comparado como el derecho internacional, a través de convenios y declaraciones, coinciden en la búsqueda de una mayor protección de los datos de carácter personal por medio de una normativa específica que cuente con un procedimiento de acceso y reclamación claro y con un órgano de control y aplicación especializado.

En este sentido, el Convenio 108 del Consejo de Europa para los Derechos Humanos al igual que toda la legislación europea dictada en la materia, prohíbe que las transmisiones de datos transfrontera sean realizadas a terceros Estados que no cuenten con una legislación específica, y con un equivalente nivel de protección o tutela del derecho a la protección de datos personales. Si Europa decidiera aplicar estrictamente su legislación de protección de datos personales al flujo de datos transfrontera, podrían quedar interrumpidas las transmisiones de datos personales entre América y Europa; inclusive aquellas de interés para los sistemas financieros, bursátiles, o bancarios, entre muchos otros.

2.5.- Evolución histórica de la idea de intimidad

Si hacemos un repaso por la historia, encontramos que el tratamiento de la información sobre las personas no es un invento moderno del hombre, ya que a lo largo de los siglos se ha transmitido información en forma permanente y de diversas formas. En la prehistoria nos encontramos con las pinturas rupestres, o, en la antigüedad, con los jeroglíficos egipcios. En definitiva, la humanidad en el

[76] Grupo de Trabajo Sobre Protección de Datos de la Unión Europea. *Dictamen 4/2002 sobre el nivel de protección de datos en la República Argentina,* (sobre el art. 29) Informe 11081/02/ES/ Final – WP 63 del 3 de Octubre de 2002, p. 14.
Fci: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp63_es.pdf (ultimo ingreso el 25/8/2012).

transcurso de la historia ha buscado siempre acumular y transmitir información, pero también ha buscado proteger su intimidad por medio del derecho. En un principio el derecho protegió ciertas manifestaciones de la intimidad. En este punto haremos un estudio de la evolución que sufrió el concepto de intimidad en la historia.

2.5.1.- Edad Antigua

En la antigüedad existieron pueblos que reconocieron determinados derechos a sus ciudadanos, cierto es que el acceso a estos derechos estaba restringido a los esclavos, a los extranjeros, a las mujeres y a todo aquel que no hubiera alcanzado el estatus de ciudadano, varón y libre.

Cuando estudiamos el derecho a la intimidad en el devenir de la historia, debemos comprender que no estamos ante una prerrogativa que nace con la protección normativa, por el contrario, estamos ante una condición inherente del ser humano, por lo que si vamos a encontrar algunas exteriorizaciones o manifestaciones de la intimidad originadas desde la intimidad del ser humano[77].

Entre estos pueblos podemos mencionar a las ciudades griegas de la Hélade. Aun así, el mundo helénico no reconoció jurídicamente a la intimidad debido al concepto globalizante y socializador de la *polis*[78], lo significativo en el mundo griego es lo público. Lo privado no es equivalente a lo particular como asimilamos hoy[79]. Los griegos no lograron configurar un derecho a la intimidad con el contenido y con la interpretación que de él se realiza en la actualidad. Sin embargo, es en la sociedad helénica en donde podemos encontrar las primeras manifestaciones de intimidad a partir de la meditación y la contemplación, prácticas que fueron valoradas por entenderse que a través de la reflexión se

[77] Basterra, M. *Derecho a la información vs. Derecho a la intimidad*. Ed. Rubinzal – Culzoni Editores. Santa Fe, 2012, p. 118.
[78] Rebollo Delgado, L. *Derecho Fundamentales y Protección de Datos*. Editorial Dykinson. Madrid, 2004, p.34.
[79] Rebollo Delgado, L. *El derecho fundamental a la intimidad*. Editorial Dykinson (2ª Edición Actualizada). Madrid, 2005, p. 52.

alcanzaba una plena vida interior, lo que representaba una íntima relación con el ser divino[80]. Para el mundo helénico, el hombre alcanzaba la sabiduría y el fundamento de su individualidad solo mediante la reflexión y el pensamiento interior. Sócrates decía "conócete a ti mismo".

Ciertamente, también existía un elemento político que atribuía un alto valor a la comunidad y la ligaba con la idea de Estado; de acuerdo con esta concepción, la existencia de un espacio reservado a la vida propiamente personal del ser humano estaba en principio excluida, ya que hasta los aspectos más interiores de la vida humana estaban controlados por el Estado y sus leyes. Esto se explica porque la sociedad griega no entendía una separación entre lo público y lo propio o personal de cada individuo, ya que todas las actividades humanas eran apéndices o participaciones de la vida en común. Tal concepción de ciudadanía fue negativa para el desarrollo y la evolución de un mundo familiar y personal, donde el individuo carecía de una vida espiritual propia y su intimidad solo se manifestaba en los pocos espacios o actividades que se desprendían de lo público. El ciudadano era partícipe activo del Estado y de su soberanía, pero carecía de una libertad negativa, que le otorgara el derecho a gozar y disfrutar de cuestiones estrictamente privadas.

El hecho de que el mundo griego no haya logrado construir un derecho a la intimidad con el alcance y contenido que actualmente tiene, no significa que el fenómeno de la intimidad o de la vida privada no existiera en la Grecia antigua. El derecho a la intimidad sí se manifestó en estos tiempos, pero fue eficazmente reprimido por la existencia de la vida común y la participación en la vida de la polis, a la cual los ciudadanos estaban obligados.

Desde la segunda mitad del siglo V a. C., la Hélade sufrió un proceso de descomposición que auguraba el fin de la comunicad política tradicional. La Guerra del Peloponeso[81], la difusión de la sofística, las luchas por el poder en Atenas,

[80] Hubeñák, F. *Historia Integral de Occidente. Desde una perspectiva cristiana*. Editorial EDUCA. Buenos Aires, 2006, p. 38.

[81] La Guerra del Peloponeso (año 431 al 404 a.C.) enfrentó a Atenas contra Esparta. Puso fin a la supremacía ateniense, aniquilando la libertad y la democracia del mundo griego.

fueron algunos de los elementos que desgastaron las tradiciones ancestrales griegas. Al comienzo de la Guerra del Peloponeso murió el 40 % de la población ateniense atacada por una cruenta peste, entre ellos el propio Pericles, el máximo estratego ateniense durante casi 30 años[82]. Todos estos factores dejaron a los ciudadanos sin la protección y sin la estabilidad que había garantizado el éxito de la vida en común dentro de la ciudad. Esta situación produjo un quebranto y un debilitamiento de la idea de soberanía que hasta ese momento se encontraba fuertemente arraigada en el pueblo griego. La decadencia de la *polis* produjo un vacío político y una angustia existencial que llevó a los hombres comunes a buscar la salvación en las religiones mistéricas de Oriente y a los intelectuales a refugiarse en morales individualistas, que respondieron a la eterna búsqueda de felicidad. Así se generaron corrientes filosóficas como los *cínicos* (que defendían la inutilidad del saber) y el vivir según la naturaleza; los *estoicos,* que hacían consistir esa felicidad en adecuarse a la naturaleza con apatía (falta de pasión) y los *epicúreos,* que defendían un placer interior consistente en la ausencia de perturbaciones (ataraxia)[83].

El descontento social provocado por la Guerra del Peloponeso y su consecuencia, el quebranto de la idea de ciudadanía, comenzó a disiparse con la aparición de sociedades religiosas o iglesias universales que encontraron su máximo exponente, siglos más tarde, en el Cristianismo. La sociedad se apoyó en nuevos ideales y escalas de valores para enfrentarse solos a los problemas y desafíos cotidianos. Entre estos nuevos valores germina una incipiente idea de intimidad, que evolucionó impulsada por la consolidación de la religión cristiana. Esta incitación social trajo como respuesta el surgimiento de nuevos valores personales y familiares sobre los que se asentaron la vida y la felicidad personal del hombre griego. La Hélade alcanzó su momento de esplendor.

Luego del apogeo del mundo griego y de la disolución del imperio de Alejandro Magno, Roma se consolidó como un poder hegemónico en Occidente y su zona de influencia fue el mar Mediterráneo. En estos tiempos, la concepción

[82] Hubeñák, F. (2006). Op. cit., p. 42.
[83] Ibidem, p. 44.

mística religiosa de la intimidad, caracterizada por el mundo griego como la búsqueda de una comunión con lo divino, desaparece. Roma, a diferencia de Grecia, realizará la distinción entre lo público y lo privado[84]. El mundo romano también entendió a la intimidad como una necesidad de cada individuo de conocerse a sí mismo y a su esencia personal, pero en general el derecho romano trató con desprecio a la intimidad, a partir de una serie de referencias normativas que declaraban ilegales los matrimonios de personas de edad avanzada porque se estimaban inútiles, o la configuración del adulterio como un delito de acusación pública.

Aun así, también existieron manifestaciones legales del reconocimiento de la intimidad, de manera que la correspondencia y el domicilio constituyeron bienes de la persona dignos de protección jurídica. Tal vez, la seguridad y el orden público, y no la idea de un debido respeto a la intimidad personal, fueron en aquel momento el fundamento principal de la protección que se dispensaba al domicilio y a la correspondencia como bienes reservados del hombre.

Ahora bien, sea como fuere, lo cierto es que la idea de intimidad adquiere mayor significación en el mundo romano que aquella que le había reconocido el mundo griego, dejando a salvo la filosofía epicúrea como un importante antecedente helénico[85].

Durante el *imperium* de Augusto nació *Jesús* "el *Cristo*", y este hecho modificó la historia de la humanidad de tal manera que dividimos los tiempos históricos en "antes" y "después" de Cristo. El hecho histórico más importante de este período fue el triunfo del cristianismo, que se convirtió sociológicamente, en la religión dominante del mundo mediterráneo.

[84] Rebollo Delgado, L. (2004). Op. cit., p.34.
[85] Herrán Ortiz, A. (1998). Op. cit., p. 6.

Si analizamos el concepto de intimidad en el mundo cristiano, encontramos en el Nuevo Testamento, en el Evangelio de San Mateo[86], un reconocimiento a la intimidad como la manifestación de Dios en la propia vida interior. El cristianismo no se limitó a una tarea evangelizadora, sino que muchos de sus seguidores prefirieron huir del mundo, que percibían corrupto y perseguidor, refugiándose en cuevas para poder consagrar sus vidas totalmente a Dios. Más tarde primó el criterio comunitario, y copiando el modelo de los apóstoles, muchos se agruparon en comunidades (*cenobios*), que fueron el origen de la vida monástica[87].

Si entendemos, como gran parte de la doctrina, que la libertad religiosa es una manifestación de la intimidad, la publicación del Edicto de Milán en el año 313, acordada por Emperadores Constantino y Licinio dio a los cristianos, como a todos los demás la libertad de seguir la religión que cada cual quiera[88]. Suprimió por completo la acusación pública de adulterio, al entender que era indigno para los matrimonios verse perturbados por la audacia de extraños[89].

2.5.2.- Edad Media

En la Edad Media estará presente al concepción cristiana del derecho a la intimidad a través de la obra de San Agustín y del redescubrimiento del Derecho Romano, junto a ello la aportación de lo propio, de la libertad del individuo frente a lo público, influirá en reconocimientos puntuales de manifestaciones del derecho a la intimidad. Esto se traducirá con posterioridad, en la manifestación concreta del derecho a la inviolabilidad del domicilio (tranquilitas domésticas) que en Castilla

---

[86] Mateo 6,3 *Cuando tú des limosna, que tu mano izquierda ignore lo que hace la derecha; 4 para que tu limosna quede en secreto; y tu Padre, que ve en lo secreto, te recompensará; 5 cuando ustedes oren, no hagan como los hipócritas: a ellos les gusta orar de pie en las sinagogas y en las esquinas de las calles, para ser vistos. Les aseguro que ellos ya tienen su recompensa; 6 Tú, en cambio, cuando ores, retírate a tu habitación, cierra la puerta y ora a tu Padre que está en lo secreto; y tu Padre, que ve en lo secreto, te recompensará*.
Fci.:http://es.catholic.net/biblioteca/libro.phtml?consecutivo=295

[87] Hubeñák, F. (2006). Op. cit., p. 85.

[88] Rebollo Delgado, L. (2004). Op. cit., p.35.

[89] Hubeñák, F. (2006). Op. cit., p. 83.

será entendida como la paz de la casa y también es reconocida por las Cortes de León de 1188[90].

San Agustín que es quién construye una idea de intimidad que la representa tal y como se la entiende en la actualidad. El gran descubrimiento, capital, de San Agustín es la intimidad. Y cuando dice: *quiero conocer a Dios y el alma*. *Nihil aliud*, (nada más, absolutamente nada más), es una fórmula que no podría emplear nunca un griego. El alma es, en definitiva, el gran descubrimiento de Agustín, el alma entendida como intimidad, lo espiritual es la realidad que es capaz de entrar en sí misma, el entrar en uno mismo es lo que da la condición de espiritual. Por eso dirá San Agustín: "no vayas fuera, entra en tí mismo: en el hombre interior habita la verdad": *Noli forasire, in teipsumredi; ininteriorehominehabitat veritas*. Esas palabras son de un enorme relieve, son de un valor incluso literario extraordinario. De eso se trata: el hombre interior. El descubrimiento es la interioridad, la intimidad del hombre. Justamente San Agustín se da cuenta de que cuando el hombre se queda en las cosas exteriores se vacía de sí mismo. Cuando entra en sí mismo, cuando se recoge en su intimidad, cuando precisamente penetra en lo que es el hombre interior, el mundo interior. Precisamente para San Agustín hay que tomar en serio que el hombre es imago Dei, imagen de Dios. Es evidente que para encontrar a Dios, lo primero, lo más adecuado será buscar su imagen, que es el hombre como intimidad, el hombre interior.

Eso es lo capital. Y toda su obra va a tener ese carácter. Uno de los libros capitales, en algún sentido el más importante, es "Las Confesiones". Y ¿qué son esas Confesiones? Es un libro que no existe en el mundo antiguo, no hay nada equivalente. Si ustedes toman algo que podría parecerse remotamente serían las Meditaciones o Reflexiones, de Marco Aurelio. Pero no es un libro de intimidad, es un libro de recuerdos, un libro de gratitud, él dice lo que debe a los antepasados, a los maestros. Esa entrada en la intimidad, en lo más profundo de sí mismo, en confesión -la palabra es confesión-, es una autobiografía. Ese es precisamente el

[90] Rebollo Delgado, L. (2004). Op. cit., p.35.

pensamiento de San Agustín: consiste primariamente en la demostración, en el descubrimiento de su propia intimidad. El hombre interior, de algún modo él lo exterioriza en un libro, en una manifestación oral, su propia intimidad. Este es el gran descubrimiento, que empieza con él, y después naturalmente va a ser adquisición de la humanidad.

En San Agustín la humanidad adquiere el sentido de la intimidad, el sentido de lo que es el hombre interior, la posibilidad de entrar en sí mismo y ahí buscar precisamente a Dios.

Durante la Edad Media, por la influencia de San Agustín, el pensamiento cristiano abandona la concepción patrimonial de la intimidad y la valoriza junto a los bienes inmateriales de la persona, a los cuales los conceptúa como un bien de la persona que, junto a la integridad física y al buen nombre, contribuyen a la plenitud existencial y a un progresivo desarrollo de las relaciones personales. La intimidad es entendida como un valor supremo de la existencia individual, y no se admite el juicio o valoración de ella, salvo cuando el interesado la ha desvelado públicamente.

El hombre es portador de valores propios y absolutos que reserva en su esfera privada. El cristianismo configuró a la intimidad como el discernimiento personal que cada individuo tiene como ser humano único, diferente y extraordinario. La reflexión y conciencia interior, el entendimiento de sí mismo y el poder de dominio sobre la propia individualidad representan las manifestaciones más sobresalientes de la intimidad como aspecto más característico de la intelectualidad humana.

Los pueblos germánicos que invadieron el Imperio romano en el siglo IV, iniciaron un lento y pausado proceso de integración que abarcó aproximadamente los siglos VI y VII.

Durante todo este lapso de denota claramente que las invasiones germanas no alteraron sustancialmente las formas de vida de la aristocracia terrateniente romana surgida tras las reformas de Dioclesiano en el siglo III. De todos modos, romanos y germanos vivían uno al lado del otro sin mezclarse ni asumir costumbres afines,

pues cada uno tenía sus propias leyes e instituciones y originariamente hasta la religión era distinta[91].

La Edad Media también se caracterizó por la influencia del viejo mundo romano y del pensamiento cristiano, que condicionaron el concepto de intimidad. En este sentido, luego de la obra de San Agustín, Tomás de Aquino marcó el dominio de la reserva en las relaciones sociales.

Tomás de Aquino considera la intimidad como un bien de la persona que se identifica con la conciencia que cada individuo tiene de ser una persona única. De esta forma, interioridad, al igual que privado, tiene un significado especial; por el contrario, intimidad es lo propio del ser humano; su conocimiento de tal individualidad, se identifica con su núcleo esencial de reflexión y vivencias. Así, la intimidad es un bien sagrado para el hombre que a nadie le es lícito invadir; tanto la capacidad intelectual como la volitiva del ser humano se encuentran en íntegra relación con la intimidad del individuo.

Durante la época feudal se mantuvo la idea de que algunos actos, comportamientos y bienes, se sustraen lícitamente a la autoridad pública y se recluyen en el dominio de las personas para mantenerse a resguardo de la intromisión ajena.

La contraposición de lo público y lo privado no se limita a una idea de localización, porque detrás de estas relaciones se traslucen cuestiones de poder y dominación. El ámbito de lo público está controlado por la comunidad, mientras que lo privado se identifica con los actos, comportamientos o vivencias personales y familiares y se regiría por el *paterfamilias*, con lo que este concepto de privacidad no estaría caracterizado principalmente por la individualidad. Sin embargo, parte del reconocimiento de la persona como un ser esencialmente libre determinado por su espíritu también libre. Los pensamientos de esa época relacionan la idea de

[91] Hubeñák, F. *Formación de la Cultura Occidental*. Editorial Ciudad Argentina. Buenos Aires, 1999, p. 197.

libertad e intimidad con el conocimiento y la libre determinación sobre su propia salvación.

En esos tiempos la intimidad se manifiesta en el derecho mediante instituciones como la inviolabilidad del domicilio, considerada un bien de la persona que alcanza un mayor desarrollo porque de la protección del domicilio se pasa directamente a la protección de la persona y de su vida familiar. El derecho a la inviolabilidad del domicilio se fundamentaba en la paz y el orden de cada rey, y en la defensa de su propio hábitat, que se traspone a la paz y al orden de la vida personal y familiar de cada individuo.

2.5.3.- Edad Moderna

En la Edad Moderna aparece la protección de la libertad de conciencia, o la moderna libertad religiosa, y se conoce el derecho a un gran número de manifestaciones de intimidad. Surgen las primeras declaraciones de derechos y las primeras constituciones modernas (Inglaterra 1688; Estados Unidos 1787, Francia 1789). España reconoce la inviolabilidad del domicilio, el secreto de las comunicaciones y la intimidad corporal[92].

La libertad, entendida como el poder de decidir que tiene cada individuo, se encuentra fuertemente relacionada con la intimidad, dado que el individuo reduce su capacidad de decidir cuando no tiene intimidad. Muchos filósofos trataron la relación entre intimidad y libertad, entre ellos Tomás Hobbes y John Locke se ocuparon en profundidad de este tema.

Lucrecio Rebollo Delgado explica que para Hobbes, el mundo se mueve entre dos fuerzas: el deseo de poder y la razón de los individuos. Para alcanzar su equilibrio es necesario un pacto, del cual surgen el Estado y la Sociedad como convenciones que se fundamentan en el individuo. A partir del pacto, el individuo sólo reserva una limitada capacidad de opción y como consecuencia se restringe su

[92] Rebollo Delgado, L. (2004). Op. cit., p.35.

ámbito de libertad e intimidad. Sólo conserva su plena libertad en todo aquello relativo a las tareas domésticas y a sus creencias; fuera de ese ámbito tiene primacía la voluntad del soberano y el individuo se transforma en súbdito. La idea de libertad hobbesiana es, entonces, negativa, dado que el individuo sólo puede decidir de acuerdo con su propio criterio cuando el soberano no ha prescripto una regla.

Aun así, la intromisión en la conciencia del individuo y en las prácticas de sus tareas domésticas solo compete a cada sujeto y quedaban vedadas para el Estado en las primeras obras de Hobbes. Sin embargo, con posterioridad cambia su forma de pensar y hace desaparecer la diferencia entre intereses domésticos y públicos, con lo que desaparece también la esfera de intimidad del sujeto que antes había defendido.

El derecho a la libertad y a la intimidad evoluciona decididamente en la obra de John Locke, dado que para este autor la ley tiene primacía sobre la voluntad del monarca y deja de ser su voluntad. De esta forma, la libertad deja de ser una libertad negativa para transformarse en una libertad positiva, puesto que la finalidad de la ley será proteger y ampliar la libertad, no suprimirla ni restringirla.

Locke desarrolla el concepto de intimidad o esfera doméstica en su obra *Carta sobre la Tolerancia* donde incluye a los asuntos privados domésticos, a la administración de propiedades y a la conservación de la salud corporal, cuestiones en las cuales el individuo puede seguir su propio camino y elegir lo que más le convenga. Conserva un ámbito de su libertad llamado privacidad, que forma parte de la actuación del individuo racional que ha superado la libertad salvaje y, por este motivo, el Estado debe abstenerse de invadir este ámbito privado de libertad del individuo. Locke indirectamente indaga sobre la intimidad al estructurar una idea de libertad que incide tanto en el derecho del individuo a reaccionar frente a presiones e influencias de los demás como en la libertad de actuar según entienda conveniente, ateniéndose exclusivamente a las normas que rigen y organizan la convivencia humana.

John Stuart Mill aporta otra interesante visión cuando profundiza en las ideas que sobre la intimidad han perfilado estos y otros autores, y defiende la existencia de un enfrentamiento entre el individuo, el Estado y la sociedad. Entiende que el individuo ha de ser libre para hacer cuanto desee, mientras no dañe al prójimo. Cada persona es por sí misma suficientemente racional para poder tomar decisiones acerca de su propio bien. El gobierno sólo debe intervenir para proteger a la sociedad, explica Mill. Diferencia dos facetas en la libertad individual: una positiva y otra negativa; la primera, consistente en la facultad del sujeto de actuar según su libre albedrío o criterio; la segunda pretende la ausencia de la intromisión por parte de los demás en las actividades que cada uno desempeña. Este autor expresa que no es lícito confundir el ámbito privado propio de la libertad humana, que toda persona es capaz de gobernar por sí misma, y el ámbito público, al que en principio los demás tienen acceso. Por eso, desde el pensamiento liberal se contempla la necesidad de proteger la esfera privada del individuo frente a las posibles intromisiones del poder público.

Los pensadores de la edad moderna superaron la concepción mística y religiosa de la intimidad. El nudo de sus reflexiones procura vincular la necesidad de la vida interior con la razón. En el hombre moderno despierta un anhelo de afirmación de su intimidad, de reivindicación de su esencialidad individual que conduce a la creencia de que este ámbito de reserva personal debe protegerse de manera más eficaz por los ordenamientos jurídicos. La propia subjetividad del individuo y su naturaleza de ser intelectual se encuentra vinculada al respeto y reserva del mundo interior de la persona; el conocimiento de si mismo, el disfrute íntimo de las experiencias, sentimientos o pensamientos constituyen un bien irrenunciable del ser humano, que lo impulsan en sus relaciones sociales, y le proporcionan dominio de su esfera interna de actuación y reflexión.

John Locke debe ser considerado uno de los pensadores más relevantes de la construcción jurídica a partir de sus reflexiones de lo que él llamó “libertades negativas”, que reconocen al individuo una esfera mínima de libertad personal, que

no pueda ser invadida por nadie y de ellas se deduce la delimitación de una frontera entre el ámbito de la vida privada y el ámbito de la actividad pública.

El comportamiento y los hábitos humanos evolucionan y en la época actual -dominada por el avance de las relaciones sociales- la intimidad adquiere nuevas dimensiones adaptándose a la realidad cambiante en cada momento. La intimidad se identifica con la vivencia individual en un mundo interior, pero también con la vivencia exterior libremente decidida por la persona. Dos decisiones personales diferentes pero complementarias caracterizan el fenómeno de la intimidad en la actualidad: por un lado, la libre determinación de "encerrarse en sí mismo" y, por otro lado, la opción consciente de abrirse a un mundo exterior y permitir el acceso de los demás a los diversos aspectos de nuestra personalidad.

No fue Rousseau quien descubrió la intimidad, sino quien la desproveyó de su fundamento personal y trascendente, reduciendo la persona a un mero individuo. El hombre antiguo no era consciente de su propia intimidad personal, pero no por ello dejó de apreciar su íntima conexión con Dios, al que tan solo encontraba a través de su interiorización intelectual. El aporte de Rousseau, y de los filósofos modernos ha sido la consideración de la intimidad desde el ámbito de la persona, sin acudir a referencias místico-religiosas para la fundamentación de una irrenunciable vida interior.

2.5.4.- Edad Contemporánea

El descubrimiento de la agricultura, durante el período neolítico[93], permitió el desarrollo de sociedades agrarias, donde la mayor parte de las comunicaciones se producían dentro de grupos muy pequeños y donde la única forma de enviar un mensaje a una audiencia masiva, era reuniendo una multitud. Era una cultura de sociedades primitivas, en la cual la multitud fue el primer medio de comunicación de masas y donde las nuevas ideas representaban una amenaza a la supervivencia,

[93] Mac Nall Burns, E. *Civilizaciones de Occidente. Su historia y su cultura*.3ª ed. Ediciones Peuser. Buenos Aires, 1953, pp. 37-38.

dado que hasta la misma noción de libertad de pensamiento era extraña a estas comunidades, que vivían al límite de la subsistencia[94].

A partir de la revolución industrial y con la aplicación de métodos de creación de riqueza basados en la masiva producción fabril, se inicia una segunda ola de cambios y transformaciones sociales que permiten el paso de la sociedad agraria a la sociedad industrial. El nuevo paradigma global exigió más comunicación a distancia y creó las condiciones necesarias para la organización de los servicios públicos de correo, telégrafo y telefonía.

La sociedad industrial diseñó medios de comunicación masivos pensados para alcanzar a una masa laboral homogénea y basados en las nuevas tecnologías de la información. Surgen grandes periódicos, revistas, cines, radios y sistemas de televisión capaces de llevar simultáneamente el mismo mensaje a millones de personas. Estos medios de comunicación masiva se constituyen en el principal instrumento de masificación del mundo industrializado.

Sin embargo, es con el advenimiento de la revolución industrial cuando el individuo ve potenciada su vida exterior y de relación con los demás, pero al mismo tiempo, toma conciencia de su necesidad de un espacio para el aislamiento y la soledad en su vida. La creciente socialización de la vida de relación plantea para la persona la urgente prioridad de garantizar un espacio de vivencias, recuerdos y pensamientos reservados al conocimiento ajeno. Cualquier manifestación individual cuenta con el rechazo de la colectividad, que paulatinamente va invadiendo tanto el espacio público como la vida privada de las personas.

Recién puede hablarse de una configuración propia del derecho a la intimidad a partir de 1890. Con anterioridad existe el reconocimiento de aspectos de la intimidad, pero no hay una concepción global del derecho, ni una conciencia de su necesidad, así como tampoco hay una delimitación propiamente jurídica. Los primeros estudios que desarrollan el derecho a la intimidad surgen en los Estados

[94] Toffler, A. (1995). Op. cit., pp. 426-430.

Unidos, al final del siglo XIX, con la doctrina de la "Privacy Law", esbozada embrionariamente en 1890 por los juristas Samuel Warren y Louis Brandeis. En ella, sus autores expresan con firmeza que la prensa ha traspasado los límites de la propiedad y la decencia, mediante la intromisión en la vida privada de las personas, tanto en el ámbito público como en su ámbito privado.

2.5.5.- Siglos XX y XXI

El siglo XX vivió los efectos de la expansión de las nuevas tecnologías de la información, las cuales generaron una tercera ola de transformaciones globales que posibilitaron el paso de la sociedad industrial a la sociedad de la información. En este nuevo escenario, el saber se transforma en el recurso que controla todo el sistema de producción, y desplaza al capital, al suelo o a la mano de obra, del lugar central que habían ocupado hasta ese momento. Los trabajadores del saber y de los servicios[95] son la nueva clase social emergente de la sociedad pos-capitalista basada en la información. El surgimiento de esta nueva clase trabajadora genera una fuerte tensión social al ir desplazando de su sitio privilegiado a la burguesía capitalista y al proletariado obrero.

Nace un nuevo sistema de creación de riqueza basado en el conocimiento y en la información, en el cual la población y la masa trabajadora emergente es mucho más heterogénea y desmasificada que la existente en la sociedad industrial. Estos nuevos actores sociales van a exigir una diversidad de mensajes, de sistemas y de medios de comunicación, antes no conocida; pensemos en Facebook, en twiter o en las redes sociales en general.

Paradójicamente, en este nuevo escenario surge un fenómeno de concentración de medios de comunicación. Mientras en la sociedad industrial los medios de comunicación operaban con más o menos independencia de los demás, al pasar a la sociedad de la información, estrechan vínculos, se fusionan entre sí, comparten datos, imágenes y símbolos, e incluso ofrecen noticias contextualizadas,

[95] Drucker, P. *La sociedad poscapitalista*. Editorial Sudamericana. Barcelona, 1999, p.15.

fraccionadas e intencionadas[96]. Los medios de comunicación se globalizan, se interconectan, se fusionan y conforman un poder de influencia social determinante. Los canales de televisión y de radio así como las publicaciones tanto en papel como en medios digitales, consideradas individualmente, lentamente van perdiendo importancia, a la par del crecimiento desmesurado de los sistemas de comunicación masiva globalizados[97].

Los sistemas de información surgidos en los últimos tiempos, potenciados por las nuevas tecnologías informáticas y su utilización en el sector de las comunicaciones, han dado origen a esta nueva sociedad basada en la dinámica del conocimiento y la información. Estos nuevos paradigmas nos presentan un proceso global de transformación, en el cual nadie nacido a partir de 1990, sería capaz de imaginar el mundo en el que nacieron sus abuelos o en el que crecieron sus padres[98].

Cierto es que la sociedad de la información también ha permitido el surgimiento de grupos desmasificados, algunos más pequeños, que reciben y se envían entre sí grandes cantidades de informaciones e imágenes, reemplazando a las grandes masas de personas que recibían la misma información, los mismos mensajes y las mismas interpretaciones de la realidad social. Surgen los blogs y los diarios digitales especializados en los cuales se observa una potente interacción de sus lectores entre ellos y con el medio.

La uniformidad en los individuos que integran una sociedad hace previsible su conducta, y por lo tanto no es necesaria tanta información, de unos sobre otros, para saber cómo se comportarán los demás. La desmasificación hace que cada individuo requiera más información para gestionar su vida y prever, con alguna aproximación, cómo se van a comportar los demás, y qué efecto tendrá ese comportamiento social sobre él. Este es uno de los motivos que explican la

[96] Terceiro, J. *Sociedad Digital. Del homo sapiens al homo digital*. Editorial Alianza, Madrid, 1996, p. 161.
[97] Toffler, A. (1995). Op. cit., p. 406.
[98] Drucker, P. (1999). Op. cit., p. 11.

constante y ansiosa búsqueda de información que cada día emprenden, tanto personas como instituciones públicas y privadas, en nuestra sociedad actual. La velocidad en la transmisión de los datos e información requerida por la sociedad se ha transformado en un valor de consumo social.

La nueva economía de la sociedad del conocimiento ha llegado a considerar más importante la distribución de la información que la distribución de la riqueza, cuestión esta que repercute directamente en una mutación de la agenda y del pensamiento político de nuestro tiempo. No hay nación que pueda gestionar una economía del siglo XXI sin una avanzada infraestructura de tecnologías de la información y de las comunicaciones, en la que interactúen sistemas informáticos de procesamiento y comunicación de datos interconectados por medio de redes de telecomunicaciones.

Peter Drucker explica que la esencia de la nueva economía es el conocimiento, y que el ideal democrático de la libertad de expresión pasa a ser una prioridad política descollante que ha dejado de ser sólo una cuestión periférica. Es precisamente por este fenómeno tecnológico, que muchos gobiernos de nuestro tiempo en su intento por conservar el poder, buscan aprovechar las TIC para sus fines e imponen límites más o menos rígidos a la libre circulación de información. En el fondo hay, muchas veces hay un vano intento autoritario de retener, como mínimo, algo de control sobre las imágenes, las ideas, los símbolos y las ideologías que llegan a la sociedad, por medio de las nuevas infraestructuras de comunicación digital.

Sin embargo, entendemos que cuanto más nos adentramos en el desarrollo de la sociedad de la información, más importante es permitir un abanico extremadamente amplio de disenso y libre expresión. Si el Estado obstaculiza el libre flujo de datos, información y conocimiento, va a estancar el avance de esta nueva sociedad en la que vivimos y va a instaurar una nueva forma de represión a la libertad de acción de las personas y al derecho a la autodeterminación informativa que hace posible el libre desarrollo de su personalidad.

El reconocimiento y la protección de los derechos y libertades de las personas, tienen un papel fundamental en la distribución del poder, en la vigencia del Estado de derecho y en la legitimidad de la democracia constitucional, principios sin los cuales esta no puede funcionar[99]. El poder de las nuevas tecnologías de la información y de las comunicaciones[100] es un elemento de fuerza que confiere a alguien la circunstancia de poseer información sobre los demás, situación que se torna cada vez más común en la sociedad de la información y que debe ser limitada por el derecho, para que no se produzcan excesos que vulneren los derechos humanos de otras personas, y en especial el derecho a la intimidad y a la protección de datos personales.

Ninguna sociedad puede tolerar una libertad de información total, ya que en la vida social es necesario algo de secreto y la libertad de información total significaría la carencia de intimidad individual. Además, es peligrosa la existencia política de un grupo social sin limitación del poder y sin respeto a un conjunto mínimo de valores que cohesionen la sociedad. Los derechos y libertades consagradas como derechos fundamentales en una Constitución, significan que cada persona puede pensar, expresar y obrar como le guste, sin otro límite que la libertad de los demás. Estas libertades pueden diferenciarse en civiles y públicas.

Las libertades civiles o libertades de la persona conciernen, especialmente a la actividad privada, pero pueden ser utilizadas también en el dominio político. Comprenden, ante todo, la seguridad o la protección contra las detenciones arbitrarias, la inviolabilidad del domicilio, la libertad de correspondencia, la libertad de residencia, el derecho a la vida y al libre desarrollo de la personalidad, el derecho a la intimidad, entre otros.

---

[99] Infantes Mandujano, P. *Constitución Política del Perú*. Editorial Librería y Ediciones Jurídicas. Lima, 1999, p. 9.

[100] Delpiano Ascencio, H. "La protección de datos personales. Bancos de Datos de Información crediticia". Editorial fcu (Fundación de Cultura Universitaria), colección JVS, Nº 47. Montevideo, 1997, p. 9.

Las libertades públicas, en cambio, se refieren a la acción colectiva, es decir a las relaciones de los ciudadanos entre sí; comprenden esencialmente la libertad de prensa y de otros medios de expresión, la libertad de reunión, la libertad de manifestación, la libertad de asociación, entre otras.

En este contexto, las garantías constitucionales constituyen un contenido esencial del orden jurídico, y entre ellas surge el *habeas data*[101] como una garantía de protección jurídica especial para los datos personales.

El surgimiento de esta nueva sociedad de la información ha supuesto una mayor invasión a la intimidad de la persona, hasta tal punto que en la actualidad el individuo reclama la adopción de instrumentos jurídicos de respuesta a las sucesivas y frecuentes intromisiones que debe padecer en su intimidad. En una sociedad caracterizada por el ansia de poder y en la que el poder se consigue con información, es lógico comprender el requerimiento del individuo en orden a la regulación de instrumentos jurídicos eficaces y adecuados para la protección de la intimidad familiar y personal.

Las formas de amenaza a la intimidad han variado y en atención a esta realidad es necesaria la adopción de medidas más contundentes y con mayor virtualidad jurídica que las existentes hasta este momento.

La intimidad no consiste únicamente en el ocultamiento o la reserva de aspectos de la vida íntima o privada de las personas, sino en el reconocimiento de un conjunto de facultades que permitan a la persona decidir respecto de su vida y de sus relaciones, disponiendo de mecanismos de defensa que aseguren la libertad del individuo y su control sobre la información que se ha revelado con respecto a su persona. Por lo tanto, los medios de defensa y protección de la intimidad que actualmente están a disposición de las personas han dejado de ser eficientes y es necesario reformularlos para salvaguardar nuestro derecho a la intimidad en su

[101] *Habeas Data*, locución latina que significa: *habed, traed tus datos.* Véase Rodríguez, A. W.; Galeta de Rodríguez, B. *Diccionario de Latín Jurídico*. *Locuciones latinas y su aplicación jurídica actual*. Editorial García Alonso. Buenos Aires, 2006.

circunstancia actual, comprendiendo que además de bienes externos, tales como la integridad física o la libertad de actuar, toda persona es también titular de otros bienes internos o inmateriales, entre los que se cuentan el honor, la intimidad o la fama.

Sin duda, ciertamente las bases o bancos de datos informáticos, no son un invento de la era tecnológica, ya que antes se utilizaban ficheros de papel o similares que constituían registros de información. La diferencia radica en que los ficheros manuales permiten almacenar información en cantidades que dependerán del espacio con que se cuente. A su vez, el sistema de búsqueda en archivos físicos es lento y engorroso, en proporción a la cantidad de información con que cuente el fichero. Por el contrario, en los ficheros o bancos de datos informatizados, el concepto de espacio y tiempo de recuperación de la información pierde importancia. La cantidad de información que puede almacenar un disco compacto es equivalente al contenido de varias bibliotecas muy pobladas, y el tiempo en que un procesador de última generación puede recuperar datos se mide en microsegundos.

Las TIC siguen avanzando día a día, actualmente la computación en nube o *cloudcomputing* permite que una gran cantidad de negocios puedan desarrollarse tan solo con un teléfono móvil, una computadora portátil y una conexión a Internet, que además se integra con el teléfono celular.

Empresas del nivel de Amazon o Google usan la computación en nube y prestan servicios basados en esta tecnología, de forma tal que cualquier organización puede acceder a aplicaciones de negocios a través de un sencillo navegador web. Esta realidad permite que cualquier usuario pueda prescindir de dispositivos de almacenamiento físico de datos (que podrían ser datos personales) y por lo tanto, ni siquiera tendría la necesidad de instalar una pequeña oficina física[102]. La oficina con la base de datos en la cual se realiza el procesamiento de

[102] Suñé Llinás, E. y Santamaría Ramos, F. (2010). Comentario de Emilio Suñé Llinás y Francisco José Santamaría Ramos al art. 43. Responsables y Encargados del Tratamiento, p. 2017. Publicado en: Troncoso Reigada A. (Director) (2010). *Comentario a la Ley Orgánica de*

datos personales, puede hoy ser como una nube que acompaña al teletrabajador donde este se encuentre.

Las nuevas tecnologías de la información han afectado todos los hábitos de la actividad humana. El mundo actualmente gira alrededor de un revolucionario universo científico y tecnológico; pero si hacemos un repaso de la historia, encontramos que también desde sus comienzos la humanidad buscó procesar y acumular información. En la antigüedad, el hombre usó el ábaco[103], un instrumento que, quizás, fue el primer dispositivo mecánico de contabilidad desarrollado por la humanidad y que no dejó de evolucionar hasta las últimas generaciones de sistemas informáticos de inteligencia artificial y robótica combinada con redes de comunicación que se distribuyen por todo el planeta.

Estamos en el principio de un proceso de evolución tecnológica en el que nuestros mejores sistemas de computadoras son tan primitivos "como un hacha de la edad de piedra[104]", y las soluciones jurídicas a los conflictos generados por estas nuevas tecnologías de la información y las comunicaciones también son rudimentarios. Por este motivo, proteger los datos personales tiene una importante incidencia sobre la legitimación política de las sociedades democráticas tecnológicamente avanzadas. Su reconocimiento supone no sólo una protección para la persona, sino también una condición del funcionamiento del sistema democrático y una garantía de legitimidad del sistema de gobierno.

Aun cuando los autores antes mencionados no atienden en forma expresa y específica al concepto de intimidad, realizan un importante aporte a la construcción del derecho a la intimidad, ya que reconocen la existencia de una esfera privada en la vida de cada sujeto, la cual necesariamente debe mantenerse alejada de cualquier intromisión, tanto del Estado como de los particulares.

Protección de Datos de Carácter Personal. Pamplona (España): Civitas y Thomson Reuters. (Editorial Aranzadi), p. 2292.

[103] Ábaco: Tabla o cuadro que sirve para el cómputo / Instrumento, artificio o gráfico destinado a resolver determinados problemas matemáticos. Se ha calculado que tuvo su origen hace al menos 5000 años y su efectividad ha soportado la prueba del tiempo.

[104] Toffler, A. (1995). *El Cambio de Poder*. Op. cit.

Desde este punto de partida, podríamos caracterizar a la intimidad por su relatividad, ya que la idea que se tiene de la vida privada puede variar de una persona a otra, de una sociedad a otra, o en función de edades, tradiciones, educación y culturas diferentes.

Sin embargo, si caracterizamos de esta forma el concepto de intimidad, estaríamos haciendo depender su contenido y su ámbito de protección, de las cambiantes circunstancias sociales, económicas y culturales de cada momento. Esta idea permitiría afirmar que en la sociedad actual la intimidad no goza de un contenido ni de un reconocimiento semejante al que se concedía en épocas anteriores, donde el desarrollo tecnológico, o bien no existía, o bien carecía de entidad suficiente para perturbar la existencia humana en sus esferas más íntimas.

La doctrina ha propuesto una fórmula evolutiva del concepto de intimidad, en la que se diferencian diversas etapas. Desde una elaboración liberal del concepto de intimidad, se configura como un "derecho a ser dejado solo", que posteriormente va a adquirir un significado más humanista, más personal, de compromiso con la protección de la dignidad humana y la defensa del individuo ante las arbitrarias injerencias externas en su vida privada.

La literatura y el cine contemporáneo también se hacen eco de este nuevo espacio vulnerable del individuo, al reflexionar sobre la intimidad en obras muy difundidas como la novela 1984 del escritor George Orwell, y esta, como tantas otras expresiones de la cultura de nuestro tiempo buscan interpretar y alertar a la humanidad sobre el significado, la vulnerabilidad y la sensibilidad de la intimidad de las personas.

Sería un error pensar que es mayor el ámbito de intimidad de una persona cuanto menos se conozca de su vida personal y familiar, ya que la intimidad no se debe vincular directamente con la reserva u ocultamiento de la información relativa a la persona; por el contrario, la intimidad debe ser ligada al libre desarrollo interior

de la vida individual de toda persona, que la faculta a desarrollarse integralmente, a conocerse y a realizarse intelectual y psicológicamente.

Es por ello que, aunque los demás penetren en la vida privada ajena conociendo aspectos de su mundo interior, a estos datos sólo acceden a través de lo que la persona les facilita, y, en cambio, les será imposible acceder al mundo interior, integrado por los más valiosos sentimientos, pensamientos y recuerdos de la persona, en los que cada individuo se recrea y proyecta como ser humano.

En resumen, podríamos decir que la intimidad constituye un bien personal al cual la persona no puede renunciar sin vulnerar y afectar su dignidad humana. El ser humano es social por naturaleza pero, pese a ello, no deja de sentir la necesidad de resguardar una vida interior distinta a las relaciones que comparte con otros individuos y que les permiten identificarse como ser humano.

De esta forma, podemos aceptar que la esencia de la intimidad no se establece sobre la sustracción de determinadas zonas de la personalidad del individuo al conocimiento ajeno, sino sobre la necesidad de proteger un ámbito de libertad interior como instrumento imprescindible para el pleno desarrollo de la personalidad individual.

Por eso se acepta que aquello que generalmente afecta a la propia intimidad, será lo que se comunique con la confianza de no ser revelado, o con la esperanza de que será utilizado en el beneficio propio de su titular.

Lo que se denomina íntimo es frecuentemente secreto o confidencial y no traspasa el reducido ámbito de las relaciones personales o familiares. Sin embargo, creemos que identificar lo íntimo con lo secreto -es decir, con aquello que es obligatorio ocultar- nos llevaría a conclusiones erradas e inaceptables para la protección jurídica que el derecho debe dar a este bien personal. Insistimos en esta idea, dado que por su propia definición aquello que es obligatorio ocultar solo puede concebirse en el más profundo e impenetrable núcleo de la persona, allí donde el acceso se encuentra cerrado a los demás y únicamente el propio sujeto

puede introducirse y dominar. Pensamos entonces que lo íntimo es diferente a lo secreto de una persona, aun cuando ciertos datos puedan, en ciertos casos, compartir esas características o calidades.

2.6.- La intimidad de las personas jurídicas

La legislación comparada reconoce, en casos puntuales, el derecho a la protección de los datos de las personas jurídicas[105]. El art. 3º, inc. b) del Convenio 108 del Consejo de Europa, de 28 de Enero de 1981, deja abierta la posibilidad de que los Estados miembros puedan extender el régimen de protección a las personas jurídicas[106].

Sin embargo, la protección de los datos personales de estas entidades ideales es un tema controvertido en las opiniones de la doctrina jurídica. El reconocimiento de la titularidad de derechos fundamentales a las personas jurídicas no es aceptado en forma unánime por los autores, con motivo de la personalidad ficticia que posee este tipo de entes.

El Tribunal Constitucional Español ha reconocido, con carácter general, la titularidad de derechos fundamentales a las personas jurídicas de derecho privado[107], al interpretar que la plena efectividad de los derechos fundamentales exige reconocer que la titularidad de ellos no corresponde solo a los individuos aisladamente considerados, sino también a grupos y organizaciones cuya finalidad sea específicamente la de defender determinados ámbitos de libertad, o realizar los intereses y los valores que forman el sustrato último del derecho fundamental. En este tema, sigue la línea de aquellos principios por los cuales los derechos fundamentales y las libertades públicas son derechos individuales que tienen al sujeto -individual o colectivo- por sujeto activo y al Estado por sujeto pasivo, en la

[105] Quiroga Lavié, H. *Habeas Data.*Editorial Zavalía. Buenos Aires; 2001, p. 43.
[106] Del Peso Navarro, E. *Ley de Protección de Datos. La nueva LORTAD*. Editorial Díaz de Santos. Madrid, 2000, p. 8.
[107] Especialmente en lo que concierne al derecho del artículo 18.2º de la Constitución Española.

medida en que tienden a reconocer y proteger ámbitos de libertades o prestaciones que los poderes deben o facilitan a aquellos.

Sin embargo, el Tribunal Constitucional Español aclara que este reconocimiento solo ser hará operativo cuando se trate de derechos que, por su naturaleza, puedan ser ejercitados por las personas jurídicas[108]. No sería ejercitable, por ejemplo, por parte de una persona jurídica, el derecho a la intimidad familiar.

La ley portuguesa de protección de datos personales Nº 67/98, de 26 de octubre[109], marcó en Europa un antecedente importante en materia de protección de datos de las personas jurídicas, luego seguido en muchas legislaciones de otros estados. La mencionada ley portuguesa expresa en el artículo 3.1, inciso b), que las personas jurídicas también son titulares de derechos, siempre que los ficheros, bases o bancos de datos contengan datos personales[110].

Siguiendo esta línea, la ley Argentina N° 25.326, en su art. 1° establece que las disposiciones de la ley de protección de datos personales también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. Es notoria la vaguedad con la cual la ley argentina trata el tema, sin establecer límite ni diferencia entre la protección que otorga a las personas físicas y aquella que extiende a las personas jurídicas. Más aún, esta ley, entiende que es titular de los datos toda persona física o persona de existencia ideal con domicilio legal o delegaciones con sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la ley[111]. Sobre este tema la doctrina Argentina no es pacífica: Peyrano[112] entiende que esta extensión del derecho a la protección de los datos personales de las personas de existencia ideal, constituye un indudable acierto, y lo fundamenta explicando que, si bien resulta indisputable que los derechos al

[108] Sentencia del Tribunal Constitucional español 64/1988 de 12 de Abril.
[109] Ley de Protección de Datos Personales Nº 67/98, de 26 de octubre (Portugal). Fci.: http://www.cnpd.pt/bin/legis/leis_nacional.htm (último ingreso 23/11/2010).
[110] Del Peso Navarro, E. (2000). Op. cit. p. 8.
[111] Ley de Protección de Datos Personales (Argentina), Nº 25.326: art. 2º.
[112] Peyrano, G. *Régimen legal de los datos personales y Habeas Data*. Editorial LexisNexis – Depalma. Buenos Aires, 200, p. 26.

honor, intimidad y dignidad personales se han considerado tradicionalmente reservados a la esfera de las personas físicas, el grado actual de evolución de la cultura jurídica se encuentra en condiciones de aceptar que dichos derechos sean compartidos (en alguna medida) por las personas no naturales; dado que algunas informaciones pueden afectar en similar medida a las personas físicas que a las de existencia ideal, sin que haya razones para excluir del derecho a la protección de datos a los grupos ideales que preservan, en idéntica dimensión, la reputación, imagen empresarial, seriedad institucional, confianza y seguridad, etcétera.

Dentro del Derecho Comunitario Europeo, el ámbito de aplicación de la Directiva 97/66[113] incluye los intereses legítimos de las personas jurídicas. La anterior Directiva 95/46 acertó al circunscribir su ámbito de aplicación a las personas físicas, pues no en vano la pretendida intimidad de las personas jurídicas puede dar lugar a la protección del secretismo de su actividad[114], cuando en realidad, el principio del derecho es la transparencia. Entiende el profesor español que la Directiva 97/66 vuelve a acertar cuando puntualmente, no sistemáticamente, protege los intereses de las personas jurídicas, en aquellos casos concretos en que son merecedores de protección, sin comprometer por ello el principio de transparencia de su actividad. Es más, incluso la distinción terminológica entre derechos de las personas físicas e intereses legítimos de las personas jurídicas, es especialmente acertada al momento de remarcar la diferencia de tratamiento, por más que desde la estricta perspectiva de la técnica jurídica sea discutible.

3.- Reconocimiento Internacional

En este punto analizaremos las fuentes -también llamadas antecedentes o reconocimientos- del derecho a la protección de datos personales y a la intimidad en el derecho internacional. Observaremos que el derecho a la protección de datos personales es una reciente creación del pensamiento jurídico de nuestro tiempo, en

[113] Unión Europea: Directiva 97/66. Esta Directiva deja fuera de su ámbito de aplicación todo aquello relacionado con la seguridad del Estado por ser esta una problemática ajena al Derecho Comunitario Europeo.
[114] Suñé Llinás, E. Op. Cit., p. 80.

consecuencia, sus antecedentes más antiguos se remontan a pocos años atrás. El primero de ellos aparece en la en el artículo 12 de la Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948, estableciendo un límite a las injerencias arbitrarias en la vida privada, la familia, el domicilio o la correspondencia de las personas[115]. El sentido de estas palabras, con relación al derecho de protección de datos personales, resulta evidente, ya que las intrusiones en la vida privada de las personas se pueden realizar a través de los modernos mecanismos de tratamiento automático de la información.

Aun cuando desarrollaremos con mayor profundidad este tema en el Capítulo II de estos estudios, podemos mencionar algunos antecedentes en el derecho europeo, por su influencia en el derecho internacional. Un primer antecedente en materia de protección de datos personales es la Conferencia de Juristas Nórdicos, celebrada en Estocolmo en mayo de 1967. Esta reunión científica tomó como referencia inmediata ciertos textos internacionales, tales como la Declaración Universal de los Derechos del Hombre, el Pacto Internacional sobre Derechos Civiles y Políticos, la Convención Europea sobre los Derechos del Hombre y representa un precedente importante, dado que reconoce que el derecho a la vida privada es el derecho de una persona a ser dejada en paz, para vivir su propia vida con el mínimo de injerencias exteriores. El alcance internacional de esta reunión de juristas es innegable, dado que acuden a ella representantes de once países, además de los pertenecientes a los países nórdicos y observadores de varias organizaciones nacionales e internacionales[116].

A su vez, se realizaron otros encuentros y reuniones científicas de gran importancia en el tema en otros lugares del planeta, entre ellos la Conferencia Internacional de los Derechos del Hombre celebrada en 1968 en Teherán, la cual, a pesar de no realizarse en Europa, influyó en el derecho europeo, porque recomienda a la ONU que proceda al estudio de las cuestiones planteadas con

[115] *Declaración Universal de Derechos Humanos*. Art. 12: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación".
[116] Herrán Ortiz, A. (1998). Op. cit., p. 55.

relación a los derechos del hombre que resulten afectados por el desarrollo de la técnica y la ciencia. En consecuencia, el 19 de diciembre de 1968 la ONU adopta la Resolución 2450, en la que establece la necesidad de fijar límites a las aplicaciones de la electrónica, por su injerencia en los derechos de la persona, y solicita al Secretario General que prepare un informe donde consten resumidamente los estudios realizados, o en curso, sobre la incidencia de las nuevas tecnologías en los derechos humanos. Se inicia así un período de intensos trabajos sobre la problemática que plantea el alcance de los progresos científicos y tecnológicos en los derechos de la persona, que concluye en 1983, con la aprobación por la Comisión de Derechos Humanos, de un informe relativo al estudio de los principios rectores pertinentes sobre la utilización de los archivos informatizados de datos de carácter personal[117].

Siguiendo este proceso evolutivo, el 23 de enero de 1970 la Resolución 428 de la Asamblea Consultiva del Consejo de Europa se refiere a la intimidad como objeto de obligada protección frente a la intromisión de la tecnología informática.

Es importante el antecedente mencionado, ya que en 1970 se aprueba en Costa Rica la Convención Americana sobre Derechos Humanos, en la que nada se declara con respecto a los peligros que acosan a la humanidad, procedentes de la abusiva utilización de las modernas tecnologías de la información.

Sin embargo, en defensa de la persona, y del libre ejercicio de sus derechos frente al progresivo desarrollo de los medios informáticos de tratamiento de la información, pronto resultan ineficaces los instrumentos jurídicos de defensa que hasta ese momento le son reconocidos con carácter general al individuo. Es decir, que los medios de defensa y prevención de injerencias en la intimidad y vida privada no eran suficientes para la protección de la persona frente a las intromisiones procedentes de una utilización abusiva o ilegítima de la informática. Solo a partir de 1976, se inicia el auge del tratamiento supranacional de la protección de la intimidad frente a la informática. Efectivamente, en 1977, la

[114] Ibídem, p. 56.

OCDE[118] auspicia un "Encuentro sobre las corrientes internacionales de datos y la protección a la intimidad de las libertades individuales"[119].

Con posterioridad, en febrero de 1978, el Comité de Política Científica y Tecnológica de la OCDE, acuerda la constitución de un grupo de trabajo específico, dependiente del Consejo, cuyo objetivo era adoptar unos criterios que pudieran unificar las políticas nacionales en los problemas del movimiento internacional de datos personales. El mandato al grupo consistió en la adopción, antes del 1º de julio de 1979, de unas directrices sobre normas básicas reguladoras del flujo internacional de datos y la protección de datos personales.

Las directrices mencionadas se aprobaron por el Consejo de la OCDE, el 23 de Septiembre de 1980, en la forma de "Recomendaciones", en las cuales, no solo se introducen recomendaciones a los Estados con respecto a la protección de datos personales en el flujo internacional, sino que se delimitan unas líneas básicas de orientación, con respecto a la protección de datos personales en el ámbito nacional o interno[120].

Este importante documento internacional tiene en su texto una relación directa con la protección de los datos de carácter personal, ya que la forma en que esas injerencias se producen en la actualidad, es a través del tratamiento automatizado de datos.

Desde mediados de los sesenta, Europa presta atención al uso de las telecomunicaciones, así como a la necesidad de una legislación que unifique

---

[118] Organización para la Cooperación y el Desarrollo Económico. La OCDE es una organización de cooperación internacional, compuesta por 34 estados, cuyo objetivo es coordinar sus políticas económicas y sociales. Fue fundada en 1960 y su sede central se encuentra en el *Château de la Muette*, en la ciudad de París (Francia). Los idiomas oficiales de la organización son el francés y el inglés. En la OCDE, los representantes de los países miembros se reúnen para intercambiar información y armonizar políticas con el objetivo de maximizar su crecimiento económico y colaborar a su desarrollo y al de los países no miembros.Conocida como «club de los países ricos», la OCDE agrupa a países que proporcionaban al mundo el 70% del mercado mundial y representaban el 80% del PNB mundial en el 2007.Fci.: http://www.oecd.org

[119] Herrán Ortiz, A. (1998). Op. cit., p. 58.

[120] Ibídem.

pretensiones y especialmente que ofrezca un conjunto de medios de protección a derechos y libertades fundamentales. No hay duda de que la legislación genérica de la Unión Europea es una legislación de mínimos en materia de protección de datos; sin embargo, ella ha permitido que los Estados miembros fueran elevando progresivamente su nivel de protección, y ha generado un efecto homogeneizador en el sistema de tutela eficaz de estos derechos.

Esta preocupación de las organizaciones supranacionales europeas en la protección de los derechos de la personalidad y en función de las lesiones que los efectos de la tecnología pueden producir en la sociedad, se formalizó en el Convenio Nº 108 del Consejo de Europa sobre la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, aprobado en 1981 y ratificado por España en 1984[121]. El Consejo de Europa es considerado el promotor de la tendencia legislativa en materia de protección de datos, superadora de los criterios que existían hasta ese momento, los cuales fueron luego adoptados por muchas leyes y por algunas constituciones europeas.

El Convenio 108 fue pionero en materia de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales. Ciertamente, su contenido no es derecho directamente aplicable, ya que está compuesto por pautas a las que deben acomodarse las legislaciones internas de países que lo han ratificado. Su texto establece una serie de principios básicos para la protección de datos, señala criterios que regulan su flujo y crea un Comité Consultivo, a quien se encomienda la formulación de propuestas para mejorar la aplicación del Convenio. Este Tratado internacional es un convenio de mínimos, ya que se trata de nociones básicas pero fundamentales. Exige que los datos sean obtenidos y procesados lícitamente, que se registren sobre la base de finalidades legítimas y que no sean utilizados de modo incompatible con esos fines. Promueve que los datos tratados sean exactos, puestos

[121] Convenio 108 del Consejo de Europa para la protección de las personas con relación al tratamiento de los datos de carácter personal (1985).
Fci.:
http://www.ifai.org.mx/pdf/ciudadanos/sitios_de_interes/datos_personales/Convenio108.pdf
También en: http://www.judicatura.com/Legislacion/1999.pdf

al día, adecuados, pertinentes y no excesivos. Recoge disposiciones acerca de los datos sensib1es, medidas de seguridad y mecanismos de cooperación internacional. Exige a las leyes nacionales que lo desarrollen, que lo apliquen en razón del territorio, independientemente de la nacionalidad de los afectados (principio de territorialidad), con el objeto de proteger a los extranjeros en igual alcance que a los nacionales de cada país.

El contenido del Convenio 108 fue tomado como un importante antecedente para la aprobación de la Directiva 95/46/CE, del parlamento europeo y del consejo de 24 de octubre de 1995[122] -relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos-. La Directiva 95/46/CE buscó armonizar la legislación europea en materia de protección de datos personales. El objetivo de esta Directiva europea aun no ha sido cumplido en su totalidad, dado que deja un amplio margen a los Estados miembros para que transpongan sus disposiciones. Esto ha provocado grandes diferencias en la legislación de los distintos Estados miembros de la UE; a modo de ejemplo, podemos mencionar el régimen sancionador[123].

Las Naciones Unidas también se ocuparon de la protección de los datos personales. La Resolución 45/1995, de 14 de diciembre de 1990, de la Asamblea General de las Naciones Unidas, recoge la versión revisada de los principios rectores aplicables a los archivos computadorizados de datos personales. Se refiere a ciertas orientaciones con respecto a datos personales y protección de los afectados que deberán llevar a cabo las legislaciones nacionales. En concreto, establece principios sobre garantías mínimas, y orientaciones sobre archivos de datos personales mantenidos por organizaciones internacionales gubernamentales. Se refiere también a archivos de naturaleza privada. Sólo son principios orientadores y

[122] Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995 (Unión Europea), relativa a la protección de las personas físicas en lo referido al tratamiento de los datos personales y a su libre circulación.
Fci.:
http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.5-cp--Directiva-97-66-CE-.pdf

[123] Suñé Llinás, E. y Santamaría Ramos, F. (2010). Op. cit., p. 2016.

recomendaciones que Naciones Unidas realizan a los Estados, y dejan a su iniciativa.

En el derecho comunitario europeo, la Directiva 95/46/CE cobra una gran importancia, dado que constituye la base del derecho de protección de datos personales en la Unión Europea.

Amplía el ámbito de aplicación del tratamiento los datos personales, ya que también incluye a los archivos o ficheros manuales, a todo tipo de soportes y formas de tratamiento de datos, tanto tradicionales como automatizados.

Con respecto a los afectados, la Directiva instaura los principios fundamentales que van a regir en adelante al derecho de protección de los datos personales: principio de calidad de datos, principio de prohibición de tratamiento de datos sensibles sin el consentimiento inequívoco y el respeto a los derechos de los afectados.

Sobre los usuarios de datos de carácter personal, la Directiva 95/46/CE establece obligaciones que deben tener en cuenta el responsable del fichero que realice tratamiento de datos personales. Determina obligaciones de gestión, organización y seguridad, que el responsable de una base o banco de datos va a tener que cumplir ante la autoridad de control o protección de datos. Determina la necesidad de cumplir con las medidas de seguridad que se establezcan al efecto, según la naturaleza de los datos, y de inscribir los ficheros de datos en el Registro que organice la autoridad de control y aplicación de la ley.

Esta norma también regula los flujos transfronterizos de datos, bajo el principio general de que el tercer país de destino de datos, debe tener un nivel de protección de datos adecuado. La Directiva excluye de su ámbito de aplicación al tratamiento de archivos relacionados con la seguridad pública y aquellos tratamientos de datos efectuados por una persona física en el ámbito de actividades personales o domésticas, sea en soporte papel o digital. Además enumera archivos a los que le dedica un régimen especial, por ejemplo los de seguridad pública,

defensa o estadística, entre otros. En España, la transposición de esta directiva implicó un cambio radical en su legislación de protección de datos personales, lo que ocurrió con la promulgación de la Ley Orgánica 15/1999, a finales de 1999.

Más tarde la Unión Europea trató la protección de los datos personales en su Constitución. El Tratado de Roma[124], es el instrumento jurídico por el que se establece una Constitución para Europa[125]; fue aprobado por unanimidad el 18 de junio de 2004, por los jefes de Estado o de Gobierno de los Estados miembros de Unión Europea. Entró en vigencia el primero de noviembre de 2006. El 29 de octubre de 2004 se procedió a la firma del tratado en Roma, donde se encuentra depositado.

Este Tratado confirma los avances logrados en materia del derecho fundamental a la protección de datos personales. Lo sitúa en el artículo II-68, dentro del Título II, que se refiere a las libertades, que a su vez se contienen en la Parte II, que lleva por título "Carta de los derechos fundamentales de la Unión"[126]. De este modo, por primera vez, la máxima norma que será de aplicación en todo el territorio de la Unión Europea reconoce expresamente el derecho fundamental a la protección de los datos personales.

Además de estos acuerdos y convenios internacionales, también podemos mencionar por fuera de la Unión Europea a los siguientes: el Pacto Internacional de Derechos Civiles y Políticos[127], la Convención Americana de Derechos Humanos

[124] Este Tratado se inspira en la herencia cultural, religiosa y humanista de los pueblos de Europa, que ha servido de base al desarrollo de los derechos inviolables e inalienables de la persona, la democracia, la igualdad, la libertad y el Estado de Derecho. Se inspira también en el avance de la civilización, del progreso y de la prosperidad. Declara su deseo de que Europa siga siendo un continente abierto a la cultura y al saber y declara como valores la solidaridad y la paz en el mundo entero.

[125] Tratado de Roma (Unión Europea). Fci: http://es.wikisource.org/wiki/Constituci%C3%B3n_de_la_Uni%C3%B3n_Europea

[126] Artículo II-68 Protección de datos de carácter personal
1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

[127] Tratado Internacional. Pacto Internacional de Derechos Civiles y Políticos. Art. 17.

(más conocida con el nombre de Pacto de San José de Costa Rica[128]), el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales[129], las Directrices para la regulación de ficheros automatizados de datos personales de la Asamblea General de las Naciones Unidas[130], las Directrices aplicables a la Protección de la Vida Privada y los Flujos Transfrontera de Datos Personales, recomendación adoptada por la Organización para el Desarrollo y Cooperación Económica (OCDE) y dirigida a los Estados Miembros y las Directrices para la armonización de la Protección de Datos en la Comunidad Iberoamericana[131].

Los mencionados son sólo algunos de los instrumentos dictados por organismos internacionales e instituciones comunitarias o supranacionales que reconocen el derecho a la protección de los datos personales como un derecho humano de tercera generación relacionado con los derechos a la intimidad, a la

---

[128] Art. 11, inc. 2º del Pacto de San José de Costa Rica: "Nadie será objeto de incidencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su hora o a su reputación".

[129] Asamblea General de las Naciones Unidas (1950). Roma: Tratado Internacional: Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales. Artículo 8: *Derecho al respeto a la vida privada y familiar. La vida privada y familiar incluye la intimidad del domicilio y la inviolabilidad de la correspondencia. Regula en qué casos puede haber una injerencia de los poderes públicos en estos derechos.*
El Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, más conocido como la Convención Europea de Derechos Humanos, fue adoptado por el Consejo de Europa el 4 de noviembre de 19501 y entró en vigor en 1953. Tiene por objeto proteger los derechos humanos y las libertades fundamentales de las personas sometidas a la jurisdicción de los Estados miembros, y permite un control judicial del respeto de dichos derechos individuales. Se inspira expresamente en la Declaración Universal de Derechos Humanos, proclamada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948. El Convenio ha sido desarrollado y modificado por diversos protocolos adicionales que han añadido el reconocimiento de otros derechos y libertades al listado inicial o han mejorado las garantías de control establecidas. Por otra parte, el número de Estados miembros se ha ido incrementando hasta abarcar casi todo el continente europeo. Su antigüedad y desarrollo lo convierten en el más importante sistema de protección de los derechos humanos en el mundo.
Fci: http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/Convention_SPA.pdf (consultado el 9/1/2013).

[130] Directrices para la regulación de ficheros automatizados de datos personales (1991). Tratado Internacional: declaración aprobada por resolución sobre la regulación de datos personales automatizados.

[131] Directrices para la armonización de la Protección de Datos en la Comunidad Iberoamericana, Bolivia (2006). Grupo de Trabajo Permanente de Desarrollo Normativo de la Red Iberoamericana de Protección de Datos. Fci.:
http://www.redipd.org/reuniones/encuentros/V/common/9_nov/Directrices_de_armonizacion.pdf

identidad, a la autodeterminación informativa y al desarrollo integral de la personalidad que existe en cada persona con fundamento en su naturaleza humana.

La importancia de afirmar que el derecho a la protección de los datos de carácter personal es un derecho humano, tal como lo hace el derecho internacional en los instrumentos mencionados, radica en las implicaciones jurídicas que esta calificación tiene para todas las personas en cualquier lugar del planeta. Al incluir a la protección de los datos de carácter personal en el catálogo de derechos humanos, excluimos toda posibilidad de que el derecho interno de cualquier Estado que respete los derechos humanos, pueda restringir o desconocer este derecho a quién reclame su aplicación, sea ciudadano o extranjero.

3.1.- Recomendación de la OCDE

En el punto anterior mencionamos que el 23 de septiembre de 1980, la OCDE dictó la Recomendación sobre circulación internacional de datos personales y la protección de la intimidad, que se centra en la adopción de medidas para aplicar al tratamiento y utilización de datos de carácter personal que comportan un riesgo para la vida privada y las libertades individuales.

Su aplicación se dirige únicamente a las personas físicas y no hace distinción con respecto a la titularidad del archivo, abarcando tanto a los archivos de titularidad pública como a los de titularidad privada.

En esta Recomendación surgen los que más tarde serían principios básicos en la protección de datos y sus correspondientes derechos para que el ciudadano pueda hacer valer aquellos reconocimientos.

La Recomendación contempla la necesidad de que la captación de los datos sea realizada por medios lícitos y legales, indicando ya en aquel entonces, que, si fuera posible, se la hiciera mediante información o consentimiento de la persona concernida.

Entre ellos se destaca el principio de la pertinencia y adecuación de los datos para el fin con el que van a ser utilizados, su exactitud y puesta al día, como también una referencia clara a la utilización limitada a las finalidades declaradas, excepto si el consentimiento de la persona afectada o una norma jurídica lo permitieren.

Se contempla el derecho de acceso a los datos dentro de un tiempo razonable, mediante un pago moderado, y el derecho a rectificar, completar o suprimir los datos inexactos o falsos, con la posibilidad de incluir sanciones y recursos en caso de inobservancia de los principios fundamentales.

Como vemos, aunque la informática ha evolucionado, y la orientación del desarrollo tecnológico ha hecho variar, en diversas ocasiones, los contenidos de las leyes de protección de datos existentes en distintos países (hoy se habla de una tercera generación de leyes de protección de datos), los principios y derechos que se recogían en estos primeros pasos siguen teniendo vigencia y actualidad, en gran parte, y solamente se trata de actualizarlos como consecuencia, en ocasiones, de la aplicación e interpretación real por los órganos jurisdiccionales de las leyes vigentes en esta materia.

En este sentido, el principio del consentimiento, reforzado como consecuencia de una Sentencia del Tribunal Constitucional alemán (ya analizada en la primera parte de esta tesis), que en 1983, dio fluidez y mayor consideración al principio de la autodeterminación informativa nota, o al "derecho de autodeterminación", centrado en el derecho de la persona a decidir cuándo y cómo está dispuesta a permitir que sea difundida su información personal o a difundirla ella misma.

Este derecho, que se enmarca dentro de los denominados derechos de la personalidad, consecuencia del ejercicio de la libertad y el reconocimiento de la dignidad humana como máxima característica de su figura, ha sido recogido posteriormente en todas las legislaciones sobre protección de datos de los países

europeos. Incluso se modificó la ley federal alemana de 1977 y luego fue recogido totalmente por la nueva ley de 1990.

En principio del consentimiento se centra hoy en gran medida la filosofía de esta protección jurídica.

4.- Técnicas legislativas aplicadas a la protección de datos

El derecho comparado nos muestra la existencia de dos sistemas o técnicas legislativas diferentes, usadas para legislar la protección de los datos de carácter personal en el mundo. Por un lado, encontramos leyes que regulan el procesamiento de datos personales por sectores de la actividad pública o privada. Otra técnica legislativa es el sistema por el cual se legisla sobre la protección de datos personales en una ley general, marco que regula toda la actividad de la sociedad, tanto pública como privada.

4.1.-Leyes Sectoriales

El sentido de las leyes sectoriales es proteger a los individuos en áreas específicas y concretas en las cuales el riesgo de tratamiento automatizado de datos personales puede tener efectos perjudiciales para la persona titular de ellos. En la legislación comparada, encontramos que Estados Unidos ha optado por una legislación de tipo sectorial que regula diversas áreas que requieren una protección particular de los datos de las personas, tales como el sector de la educación, el sector de los tributos fiscales, el sector de la salud, el sector de la seguridad entre muchos otros. Este tipo de legislación sectorial carece de una protección general de los datos personales, y solo garantiza la protección de los datos personales en ciertas actividades reguladas por normas particulares y específicas de ese rubro. En este modelo de legislación no existe un sistema general y completo de protección de datos personales, y aun cuando, en el tiempo, el legislador pueda ir completando con leyes sectoriales todas las áreas que considere peligrosas para la exposición de los datos personales de una persona, la inexistencia de una norma superior privará al

sistema normativo de un cuerpo sistémico de principios generales que resuelvan aquellas situaciones que la realidad y la evolución de la tecnología produzcan, sin que el legislador las hubiere previsto.

La técnica de regulación sectorial, también carece de una autoridad reguladora pública específica para la protección de los datos de carácter personal, sea o no independiente, que vele por la protección general de los datos personales. Esto es así porque la legislación sectorial, al no legislar en forma genérica y horizontal sobre todo lo relativo a los datos de carácter personal, difícilmente pueda crear un organismo que como autoridad de aplicación exceda el objeto de la propia ley que lo crea. Como resultado, se produce una pulverización de competencias tutelares en esta materia, referida al derecho a la protección de datos de carácter personal, área que -como ya mencionamos- por su relación con las nuevas tecnologías de la información y de las telecomunicaciones, requiere de técnicos y especialistas con alta preparación específica en la temática. Difícilmente una organización estatal no específicamente diseñada para la protección de los datos personales, pueda contar con estos recursos y capitalizar las experiencias de su personal.

4.2.- Leyes Ómnibus

En el derecho parlamentario encontramos una técnica diferente al sistema de las leyes sectoriales, en la legislación de tipo ómnibus. Este sistema normativo se basa en la búsqueda de una protección legislativa general de los datos de carácter personal, mediante el dictado de una ley que contenga una enunciación de principios genéricos en la materia, y en general, este sistema también crea una institución a la que se designa como autoridad de aplicación con poder de policía tutelar. Este modelo normativo fue el elegido por los diferentes Estados europeos en un primer momento en las primeras leyes promulgadas en la materia, y luego por impulso de la misma Unión Europea, que estableció en la directiva 95/46/CE la obligatoriedad, para los estados miembros, de legislar sobre la protección de datos

personales, mediante este tipo de sistema de normas o leyes ómnibus y de establecer una autoridad de aplicación y control específica.

En un sistema de legislación ómnibus de protección de datos personales, podemos encontrar las siguientes características: 1) existencia de reglas sustantivas generales aplicables al tratamiento automatizado de datos relativos a personas identificadas o identificables; 2) atribución de derechos a las personas titulares de los datos y de obligaciones a las personas responsables del fichero; 3) disposiciones especiales en el almacenamiento, colección, procesamiento y trasmisión en los datos de carácter personal; 4) creación de una autoridad competente encargada de vigilar la aplicación de la ley.

Sin embargo, podemos aceptar que la debilidad del modelo de protección normativa por medio de leyes ómnibus, se encuentra en la rigidez propia del mismo sistema, que a veces impide amoldarse a nuevos desarrollos tecnológicos. Pero en realidad, esta crítica también vale para el sistema sectorial en general y, en particular, en aquellas situaciones de lagunas normativas, o sectores sobre los cuales no se ha legislado.

La doctrina jurídica estadounidense defiende la protección de datos de carácter personal mediante un sistema normativo sectorial, fundándose en que las leyes de tipo ómnibus son un conjunto de técnicas destinadas a obstaculizar las relaciones comerciales internacionales, que impiden el libre flujo de información.

5.- Habeas Data

Al recorrer la evolución histórica del derecho a la protección de los datos personales y del derecho a la autodeterminación informativa, encontramos que estos derechos se desarrollaron en forma diferente en Europa y en América.

En Europa observamos que el desarrollo del derecho a la protección de los datos personales comienza primero en las constituciones o en la legislación[132], para llegar después a la jurisprudencia[133] y, a partir de su influencia, la evolución de las distintas generaciones de leyes dar que finalmente serán uniformadas por el derecho comunitario en la Directiva 95/46/CEE y sus modificatorias.

En cambio, el derecho del continente americano, especialmente en América Central y en América del Sur, el desarrollo de este derecho surge con la introducción de un derecho, facultad o garantía de acceso a los datos personales, en las constituciones de los distintos Estados de la región. La primera que lo incorpora es Brasil, en la reforma Constitucional de 1985, al introducir en su texto un novedoso instituto, al que va a dar el nombre de *habeas data*. Es importante observar la influencia del derecho comparado europeo, dado que dos años antes, en 1983, el Tribunal Constitucional alemán había dictado su célebre sentencia sobre la Ley del Censo, por medio de la cual madura la doctrina de la autodeterminación informativa.

Las constituciones del Centro y Sur de América fueron incorporando en sus reformas constitucionales producidas a partir de 1980 esta facultad, o garantía constitucional de habeas data[134], que constituye, en suma, un cauce procesal constitucional para salvaguardar la libertad de la persona ante la acumulación y procesamiento informático de sus datos personales.

Esta nueva garantía constitucional busca, desde su concepción subjetiva o derecho a la autodeterminación informativa, dar amparo al ejercicio del derecho a la intimidad informática y otorga a toda persona el derecho a controlar sus datos personales por medio de una acción procesal concreta, expedita y rápida, que toma la forma de una especie de amparo.

---

[132] Ley del Land de Hesse, Alemania, 1973.
[133] STCA (Alemania), sobre la ley del Censo (1983).
[134] Ekmekdijan. A.; Pizzolo C. (1996). Op. Cit., p. 10.
Pérez Luño, A.*Derechos Humanos, Estado de Derecho y Constitución*. Quinta Edición. Editorial Tecnos, Madrid. 1995, pp. 321-324.

Luego de la introducción de esta garantía constitucional, surgirán en América las leyes de protección de datos personales, por influencia del derecho comparado europeo y como una lógica consecuencia de una necesidad social.

El *habeas data* es la consecuencia de dotar de un procedimiento específico al derecho a la autodeterminación informativa, para proteger los datos personales por medio de un procedimiento establecido en la Constitución para garantizar al afectado, el ejercicio de su facultad de solicitar información sobre su persona, y ejercer un efectivo control sobre ella.

A este procedimiento se conoce con el nombre de *habeas data*. Su planteo puede ser extrajudicial, por medio de notificación fehaciente ante quien pueda tener datos sobre el afectado, o también judicial, en un proceso de amparo al derecho personalísimo a la autodeterminación informativa, reglado por normas procesales específicas, contempladas primero en la Constitución y luego desarrolladas en una ley sobre la materia. Es necesario destacar que la ausencia del desarrollo legislativo de la norma constitucional no priva de operatividad a este instituto.

Esta garantía constitucional se encuentra actualmente incorporada en la mayoría de las constituciones americanas para la protección de los datos personales de las personas. Es en concreto el derecho que tiene toda persona a solicitar vista sobre los datos que a ella se refieren, y en caso de falsedad, desactualización o situación de discriminación, real o potencial, a solicitar la eliminación, supresión, confidencialidad o actualización de tales datos.

El nombre de *habeas data*[135], surge por primera vez en la Constitución de Brasil del año 1985, a partir de la combinación de palabras que vienen del latín: *habeas*(traer) y data (dato en inglés). Traer el dato o los datos al titular o afectado que solicita conocer la información que existe sobre él en un banco o base de datos.

[135] *Habeas Data*: locución latina, viene de habed, tened (tus) datos. Ver: Diccionario de Latín Jurídico (2006).Op. Cit.

El desarrollo de estos derechos y garantías a la protección de datos de carácter personal son altamente sensibles a los avances tecnológicos. Por este motivo, su evolución requiere una permanente dinámica para poder acompañar los avances tecnológicos y las transformaciones que su uso genera en la sociedad.

La acción de habeas data se define como el derecho que asiste a toda persona -identificada o identificable- a solicitar judicialmente la exhibición de los registros -públicos o privados- en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoleto o que impliquen discriminación. Constituye, en suma, un cauce procesal para salvaguardar la libertad de la persona ante la acumulación y procesamiento informático de sus datos personales.

6.- Jurisprudencia del Tribunal Constitucional español sobre protección de datos

El Tribunal Constitucional español ha tenido un destacado papel en la tutela de los derechos humanos en general, y en particular del derecho a la autodeterminación informativa y a la protección de los datos de carácter personal al resolver recursos interpuestos por vía del art. 53.2 de la Constitución Española.

Probablemente por influencia del art. 18 de la Constitución Española, la primera etapa en la jurisprudencia del TC se ocupó de poner límites a la informática para proteger la intimidad personal y familiar. Su primer pronunciamiento en este sentido fue la Sentencia 254/1993, y a partir de ella, distintos fallos confirmaron esta doctrina.

Posteriormente, el 30 de noviembre del 2000, el TC marcó un punto de evolución en su jurisprudencia con las coetáneas y memorables STCs 290 y 292/2000 que al ampliar su tutela a la libertad informática, son para la doctrina la

inevitable referencia al derecho a la autodeterminación informativa, y a su definición[136].

La influencia del TC no sólo alcanzó a la jurisprudencia y a la doctrina de los autores del derecho español y comparado, sino que también se hizo patente en la legislación, que, coincidiendo con su hermenéutica jurídica en la materia, eliminó la mención que hacía la LORTAD sobre los datos automatizados para extenderse en la LOPD a todo tipo de datos susceptibles de tratamiento, sin distinguir el soporte físico en el que se encuentren resguardados.

Hecha esta breve introducción, avancemos en el análisis de cada una de estas Sentencias por separado:

6.1.- Sentencia 290/2000 de 30 de noviembre

Luego de un profundo estudio del tema, los jueces del Tribunal Constitucional revisaron en un maratónico 30 de noviembre de2000 la constitucionalidad de determinados artículos de la LORTAD (Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de Datos de 29 de Octubre), impugnados unos por motivos sustantivos y competenciales.

La sentencia 290/2000 resuelve los recursos de inconstitucionalidad acumulados e interpuestos por el Consejo Ejecutivo de la Generalidad de Cataluña, el Parlamento de Cataluña y D. Federico Trillo-Figueroa Conde en representación de cincuenta y seis Diputados del Grupo Parlamentario Popular contra los artículos 6.2, 19.1, 20.3, 22.1 y 2, 24, 31, 39.1 y 2, 40.1 y 2 y la Disposición Final Tercera de la Ley Orgánica 5/1992. Los planteos basados en motivos sustantivos objetaron la

[136] Rebollo Delgado, L. (2005). Op. cit. p. 174.

vulneración de los artículos 16.2[137] y 18.1 y 4, en relación con los artículo 10.1 y 2[138] , 53.1 y 105 b) de la Constitución Española.

A pesar de la histórica referencia del 30 de noviembre, el Tribunal Constitucional debatió largamente estos recursos, a tal punto que el tiempo transcurrido desde su planteo en el año 1993 hasta la sentencia del año 2000, alcanzó para la derogación de la norma en vigencia y la promulgación de la LOPD, nuevo texto legal que vino a derogar parcialmente a la LORTAD, norma impugnada en estos recursos.

Por este motivo, el TC declaró que no podía pronunciarse en abstracto sobre eventuales tachas de inconstitucionalidad a la LORTAD, dado que tras la derogación de la norma se había operado la pérdida del objeto de los recursos, ya que los artículos refutados no podían producir efecto en lo relativo a situaciones posteriores. Por esta vía el TC sorteó los recursos sustantivos y ocupó el resto de los enjuiciamientos a las tachas de inconstitucionalidad que aquejaban al reparto competencial entre el Estado y las Comunidades Autónomas, estimando que la deliberación del asunto exigía el previo examen del contenido del derecho fundamental a la protección de los datos personales, y a tal fin, tomó como punto de partida el fundamento jurídico sexto de la STC 254/1993 de 20 de julio.

6.2.- Sentencia 254/1993 de 20 de julio

En la STC 254/1993 el Tribunal Constitucional español se ocupó de examinar la constitucionalidad de la denegación presunta por parte del Gobernador Civil de Guipúzcoa y del Ministerio del Interior a la solicitud del actor relativa a la

[137] Constitución Española. *Artículo 16.2*: Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

[138] Constitución Española. *Artículo 10.1*: La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la Ley y a los derechos de los demás son fundamento del orden político y de la paz social. *Artículo 10.2*. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los Tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

comunicación de la información sobre sus datos de carácter personal existentes en ficheros automatizados de la Administración del Estado.

Denunciada la mora y elevada el alza ante el Ministerio del Interior con idéntico resultado, el interesado interpuso recurso judicial que fue desestimado en las dos instancias. Finalmente combatió la negativa judicial ante el TC, solicitando amparo a la luz de lo dispuesto en el Convenio 108 del Consejo de Europa de 28 de enero de 1981 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.

Además, el solicitante de amparo invocó el artículo 18.4 de la CE[139], conforme al criterio de refuerzo de los derechos a la propia imagen y a la intimidad, reconocidos en el artículo 18.1 del texto constitucional. La demanda subrayó la necesidad de proteger a los ciudadanos frente al peligro que supone el uso de la informática, y la obligación de dirigir al legislador un mandato para que limitase su utilización. Concedido el trámite de audiencia al Ministerio Fiscal, este informó a favor del otorgamiento del amparo solicitado, fortaleciendo los alegatos en torno al art. 18.1 y 4 de la C.E.[140] con la mención al derecho al acceso de los ciudadanos a los archivos y registros administrativos, en los términos del art. 105.b[141] de la Constitución Española.

El TC acoge los argumentos de aquellas dos partes, y desecha, en cambio, los mantenidos por el Abogado del Estado. De este modo valora negativamente la potencial agresividad que los avances tecnológicos infligen sobre los más elementales derechos de la persona a consecuencia del uso indebido de bancos de datos, hasta el punto de irradiar el valor del derecho contenido en el artículo 18.4 de

---

[139] *Constitución Española. Artículo 18.4*: La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

[140] Constitución Española. *Artículo 18.1*: Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. *Artículo 18.4*: La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

[141] Constitución Española. *Artículo 105*: *La Ley regulará: … b. El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.*

la CE, más allá de la sola garantía que su letra ejerce sobre el derecho al honor y a la intimidad. Intuye, en consecuencia, que el derecho a la protección de datos encierra "algo más" que el refuerzo al honor y a la intimidad de las personas en el pleno ejercicio de sus derechos. Sin embargo, condiciona el uso de la informática al respeto de algunos derechos clásicos, sin considerar realmente la existencia de un nuevo derecho fundamental, que ahora conocemos como "derecho a la autodeterminación informativa". Sin embargo, resulta indiscutible el alcance de esta sentencia precursora, aun cuando reduce sus contornos al derecho a la intimidad. En esos tiempos, la doctrina trabajaba en la construcción de un derecho distinto y autónomo, capaz de poner un límite a la intromisión informática en la intimidad de las personas.

En el fundamento jurídico sexto de la Sentencia 254/1993, el TCE expresa que la adecuación de una norma legal -o de una disposición o actuación de los poderes públicos- a lo preceptuado por un tratado internacional, y por consiguiente, el hecho de que las autoridades españolas hubieren cumplido o no los compromisos derivados de un acuerdo internacional, son cuestiones que, consideradas en sí mismas, resultan indiferentes para asegurar la protección de los derechos fundamentales comprendidos en el art. 53.2 C.E.[142], que es el fin al que sirve la jurisdicción del Tribunal Constitucional en el ámbito del recurso de amparo.

En esta línea, el TCE manifiesta que los textos internacionales ratificados por España pueden desplegar ciertos efectos en relación con los derechos fundamentales, en cuanto pueden servir para configurar el sentido y alcance de los derechos recogidos en la Constitución y hace referencia a lo antes expresado en la STC 38/1981, fundamentos jurídicos 3. y 4, en virtud del art. 10.2 C.E.[143] Desde

[142] Constitución Española. Artículo 53.3: El reconocimiento, el respeto y la protección de los principios reconocidos en el Capítulo III, informará la legislación positiva, la práctica judicial y la actuación de los poderes públicos. Sólo podrán ser alegados ante la Jurisdicción ordinaria de acuerdo con lo que dispongan las Leyes que los desarrollen.

[143] Constitución Española. Artículo 10.2: Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los Tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

esta perspectiva, el T.C. examina la demanda de amparo resuelta en la STC 254/1993.

En su doctrina expresa que el art. 18.4 C.E. dispone que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Así, la Constitución Española incorpora una nueva garantía constitucional en respuesta a una nueva amenaza concreta a la dignidad y a los derechos de la persona, y lo hace de manera similar al modo en que fueron originándose e incorporándose históricamente los distintos derechos fundamentales.

En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente los derechos al honor y a la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, a lo que la Constitución Española llama "la informática".

Es importante contextualizar que el TC se encuentra con el problema de que en el año 1990, momento de los hechos que dan lugar a la demanda, existía en España ausencia de un desarrollo legislativo sobre el derecho a la protección de datos. Sin embargo, interpreta que ante la laguna legislativa no se pueden permitir las desmesuradas consecuencias que postula el Abogado del Estado. Y aun en la hipótesis de que un derecho constitucional requiera un desarrollo legislativo para alcanzar operatividad, desarrollo y plena eficacia, la jurisprudencia española ya había negado que el reconocimiento constitucional tenga otra consecuencia que la de establecer un mandato dirigido al legislador sin virtualidad para amparar por sí mismo pretensiones individuales. En otras palabras, niega que los derechos constitucionales sólo sean exigibles después que el legislador los haya desarrollado. Esta doctrina ya había sido pronunciada por el TC en sendas sentencias, donde expresaba que los derechos y libertades fundamentales vinculan a todos los poderes

públicos, siendo origen inmediato de derechos y obligaciones, y no meros principios programáticos. Este principio general de aplicabilidad inmediata no sufre, para el TC, más excepciones que las que imponga la propia Constitución, expresamente o bien por la naturaleza misma de la norma (STC 15/1982[144], fundamento jurídico 8[145]).

Hay que destacar el voto del Magistrado Manuel Jiménez de Parga y Cabrera en la STC español 290/2000, ya que, aun cuando el ponente de la sentencia haya sido el Magistrado González Campo, el voto particular de su par Jiménez de Parga y Cabrera fue el más sustancioso en lo que hace a la doctrina del derecho a la protección de datos personales.

---

[144] STC (España) 15/1982.
Fci.: http://www.boe.es/buscar/doc.php?coleccion=tc&id=SENTENCIA-1982-0015

[145] STC (España) 15/1982. Fundamento Jurídico 8: De ello no se deriva, sin embargo, que el derecho del objetor esté por entero subordinado a la actuación del legislador. El que la objeción de conciencia sea un derecho que para su desarrollo y plena eficacia requiera la *interpositiolegislatoris* no significa que sea exigible tan sólo cuando el legislador lo haya desarrollado, de modo que su reconocimiento constitucional no tendría otra consecuencia que la de establecer un mandato dirigido al legislador sin virtualidad para amparar por sí mismo pretensiones individuales. Como ha señalado reiteradamente este Tribunal, los principios constitucionales y los derechos y libertades fundamentales vinculan a todos los poderes públicos (arts. 9.1 y 53.1 de la Constitución) y son origen inmediato de derechos y obligaciones y no meros principios programáticos; el hecho mismo de que nuestra norma fundamental en su art. 53.2 prevea un sistema especial de tutela a través del recurso de amparo, que se extiende a la objeción de conciencia, no es sino una confirmación del principio de su aplicabilidad inmediata. Este principio general no tendrá más excepciones que aquellos casos en que así lo imponga la propia Constitución o en que la naturaleza misma de la norma impida considerarla inmediatamente aplicable supuestos que no se dan en el derecho a la objeción de conciencia. Es cierto que cuando se opera con esa reserva de configuración legal el mandato constitucional puede no tener, hasta que la regulación se produzca, más que un mínimo contenido que en el caso presente habría de identificarse con la suspensión provisional de la incorporación a filas, pero ese mínimo contenido ha de ser protegido, ya que de otro modo el amparo previsto en el art. 53.2 de la Constitución carecería de efectividad y se produciría la negación radical de un derecho que goza de la máxima protección constitucional en nuestro ordenamiento jurídico. La dilación en el cumplimiento del deber que la Constitución impone al legislador no puede lesionar el derecho reconocido en ella. Para cumplir el mandato constitucional es preciso, por tanto, declarar que el objetor de conciencia tiene derecho a que su incorporación a filas se aplace hasta que se configure el procedimiento que pueda conferir plena realización a su derecho de objetor, declaración, por otra parte, cuyos efectos inmediatos son equivalentes a los previstos en el Real Decreto 3011/ 1976, de 23 de diciembre, ya que, según advierte el Abogado del Estado, la Presidencia del Gobierno no está haciendo uso en el momento presente de la autorización en él contenida en relación con la prestación social sustitutoria. No corresponde, sin embargo, a este Tribunal determinar la forma en que dicha suspensión o aplazamiento ha de concederse, por lo que no puede proceder, como pretende el recurrente en su escrito de demanda, a la adopción de las medidas adecuadas para que el Ministerio de Defensa y sus órganos subordinados le concedan la prórroga de incorporación a filas de cuarta clase a).

La STC 290/2000 profundiza su razonamiento, puesto que el art. 18.4 de la Constitución Española es revalidado por el Tribunal Constitucional como un instituto de garantía de otros derechos, enlazados principalmente a la intimidad y al honor, pero que se manifiesta además como un derecho o libertad fundamental frente a las potenciales agresiones que el uso incontrolado de la informática causa sobre la dignidad y la libertad de la persona. La garantía de esta intimidad exige a favor del individuo el poder de control y disposición sobre sus datos personales.

Cuando el fallo interpreta que la libertad informática constituye el derecho a controlar el uso de los datos relativos a la persona insertos en un programa informático, se interna en el terreno del *habeas data*, y comprende, entre varios aspectos, el derecho a consentir la recolección de datos y su tratamiento. En otras palabras, el artículo 18.4 de la Constitución Española reconoce el derecho a la autodeterminación informática al limitar el uso de las nuevas tecnologías en garantía del honor, de la intimidad personal y familiar de los ciudadanos y del pleno ejercicio de sus derechos.

Ahora bien, si es cierto que este derecho es pacíficamente reconocido desde la STC 254/1993, su vinculación con la intimidad personal del individuo ha variado en los sucesivos pronunciamientos jurisprudenciales, hasta llegar a un nuevo estándar jurisprudencial con la STC 290/2000 en el voto particular suscripto por el Magistrado Jiménez de Parga y Cabrera, al cual se adhirió el Magistrado Rafael de Mendizábal Allende. Los argumentos doctrinales desarrollados en este voto particular contribuyeron a consolidar el derecho a la libertad informática desde un concepto autónomo que configura un nuevo derecho fundamental, cuya protección no figuraba en el texto de la Constitución Española de 1978.

Jiménez de Parga y Cabrera esgrime la posibilidad de incorporar un nuevo derecho al listado oficial de los derechos fundamentales, sin el paraguas de una cláusula abierta. Por este motivo es que recuerda que la STC 254/1993 mencionó por primera vez en la Jurisprudencia española la libertad informática entendida como un derecho fundamental, en sí mismo considerado. De modo que con el

propósito de tutela a un derecho esencial no contemplado por el constituyente, el TC forzó su construcción sobre la base del artículo 18.4 de la Constitución española, aun cuando esta norma había sido concebida como un mero refuerzo a los derechos contenidos en el artículo 18.1.

En la doctrina española también hay opiniones contrarias a la tesis del voto particular del Magistrado Jiménez de Parga y Cabrera pronunciado en la STC 290/2000. La doctrina divergente niega la existencia de un *numerus apertus* de derechos fundamentales, dado que los constituyentes incluyeron el apartado 4 del artículo18 de la Constitución Española con la función de garantizar a su titular un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado.

Si bien es cierto que el control del tráfico de los datos de carácter personal cobra verdadera importancia en el marco de las nuevas tecnologías, la autodeterminación informativa extiende su protección a los datos personales registrados en cualquier tipo de soporte físico, sea cual fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. En consecuencia, gran parte de la doctrina entiende que la autodeterminación informativa no puede constreñirse al uso de las nuevas tecnologías, aun cuando estamos de acuerdo en que su limitación es esencial en el ejercicio del derecho.

De esta forma, el artículo 18.4 no debiera ser considerado más que un instrumento de ayuda, tanto a la defensa de la intimidad y del honor como del *habeas data*. Por este motivo es preferible denominar a este instituto como el derecho a la libertad o autodeterminación informativa, más que la originaria expresión libertad informática.

Este razonamiento encaja correctamente con el voto particular del Magistrado Jiménez de Parga y Cabrera, ya que su autor entiende que la libertad informática debe tener un eje vertebrador, en el art. 10.1 de la CE, ya que es un derecho inherente a la dignidad de la persona. Y es esta vinculación a la dignidad de la

persona la que proporciona a la libertad informática la debida consistencia constitucional, si bien colaboran en su perfil los derechos al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1 de la C.E.) y la libertad de expresión y de información (art. 20.1 de la C.E.); así como los Tratados y Acuerdos internacionales, en cuanto son guía de interpretación constitucional (art. 10.2 de la C.E.).

Como vemos, la dignidad de la persona, consagrada en el art. 10.1 de la C.E., pasa a tener una especial relevancia y se convierte en la piedra de toque del *habeas data*. La dignidad humana se erige entonces en el soporte esencial de cualquier valor inherente a ella, y convierte los principios constitucionales recogidos en el precepto, no sólo en informadores de todo el ordenamiento jurídico, sino además en fuente normativa inmediata, lo que posibilita el desarrollo jurídico con la construcción de un derecho nuevo, tutelable por el orden constitucional.

6.3.- Sentencia 292 de 30 de noviembre de 2000

En el punto anterior vimos cómo la STC 290/2000 evitó pronunciarse sobre los recursos sustantivos interpuestos en el año 1993 contra parte del articulado de la LORTAD.

La entrada en vigor de la LOPD en 1999, supuso la protección definitiva de los datos de la persona física, dado que esta norma estableció rígidos límites a la circulación de los mismos bajo el compromiso legal de conciliar los valores fundamentales del respeto a la vida privada y a la libre circulación de la información entre los pueblos.

Sin embargo, se dio la circunstancia de que la ley derogadora incluía nuevamente en su cuerpo normativo ciertos límites al derecho de los ciudadanos a consentir la cesión de los datos personales entre administraciones públicas, para fines distintos de los que motivaron inicialmente su recolección. La respuesta social no se hizo esperar y una vez más el Defensor del Pueblo interpuso el recurso de

inconstitucionalidad 1463-2000[146], ante el Tribunal Constitucional respecto de los artículos 21.1 y 24.1 y 2 de la LOPD. El Defensor del Pueblo hizo constar, en su recurso de inconstitucionalidad, que la nueva ley reproducía los preceptos que fueron objeto de recursos en el año 1993, sin que existieran variaciones jurisprudenciales o normativas relevantes posteriores a esa fecha.

De forma tal que aquella STC 290/2000, conocedora de la inconstitucionalidad de la LORTAD, no fue más que un capítulo procesal que trasladaba la solución a otra Sentencia pronunciada el mismo 30 de noviembre del mismo año, con el número de referencia 292 y bajo la ponencia de igual Magistrado, pero con la asunción básica de las consideraciones vertidas en el voto particular de Manuel Jiménez de Parga y Cabrera, comentado *ut supra*.

Al dictar la STC 292/2000, el Tribunal Constitucional declaró inconstitucionales y nulos el inciso 1 del artículo 21 de la LOPD[147], que expresa: "cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso", y el apartado 1 del artículo 24, "impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas" y "o administrativas", junto con todo el apartado 2 de dicho artículo: "Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase

[146] Defensor del Pueblo (España). Recurso de Inconstitucionalidad 1463-2000 interpuesto por el Defensor del Pueblo. Fci.:http://www.boe.es/buscar/doc.php?id=BOE-A-2000-6745(ultimo ingreso el 20/1/2013).

[147]LOPD. Ley Orgánica de Protección de Datos de Carácter Personal (España), Ley 15/1999 de 13 de Diciembre. Fci.: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf
Artículo 21. Comunicación de Datos entre Administraciones públicas. *Inciso 1°*): Los datos de carácter Personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia Española de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas."

Los preceptos de la LOPD impugnados por el Recurso de Inconstitucionalidad 1463-2000 presentado por el Defensor del Pueblo y resuelto en la Sentencia analizada, hacen referencia a la cesión de datos entre administraciones públicas y a las condiciones en que las mismas se pueden producir. Estos preceptos estaban dirigidos a facilitar los datos y su comunicación en el seno de las Administraciones públicas, bajo la justificación de resultar necesarios para su buen funcionamiento.

La STC 292/2000 es un verdadero hito para la interpretación jurídica de la protección de datos personales. La sentencia diferencia plenamente la intimidad (criterio fundado en la STC 254/1993 y mantenido por la jurisprudencia posterior) de la privacidad, uno de cuyos instrumentos se encuentra en el art. 18.4 de la C.E., pero que se sustenta sobre la dignidad del ser humano al garantizar a todas las personas el derecho a conocer qué datos suyos están en posesión de terceros y para qué los utilizan.

Esta sentencia del TC español afirma que el contenido del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueden afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, ya que para ello existe la protección que el art. 18.1 de la C.E. otorga. Por el contrario, su objeto son los datos de carácter personal.

También esta Sentencia sostiene que el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue del derecho a la intimidad personal y familiar del art. 18.1 de la C.E. Dicha singularidad radica en su

contenido, ya que, a diferencia del derecho a la intimidad, que confiere a la persona el poder jurídico de imponer a terceros la obligación de abstenerse de toda intromisión en su esfera íntima y la prohibición de hacer uso de lo así conocido. En cambio, el derecho a la protección de datos atribuye a su titular un haz de facultades cuyo ejercicio impone deberes jurídicos a terceros, que actúan al margen de la intimidad, y que gravitan en torno al control de los datos relativos a su persona. De ahí se deriva la necesaria limitación del almacenamiento de los datos en archivos o bancos de datos y su posterior circulación, que sólo podrá realizarse cuando sea legalmente exigible, cuando se derive de la actividad pública del titular y puedan ser recogidos de fuentes accesibles al público, o bien cuando medie autorización voluntaria y expresa del afectado.

Esta limitación sirve a la capital función que desempeña este derecho fundamental, descripta por la STC 292/2000 como dirigida a "garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer".

El derecho a la protección de datos implicará, a partir de esta sentencia, el ejercicio de otros derechos de carácter no fundamental pero complementarios e instrumentales del mismo, tales como la prestación o revocación del previo consentimiento para la recogida y uso de los datos personales, de información sobre el destino y uso de esos datos, así como los derechos de acceso, rectificación y cancelación.

En definitiva, el reconocimiento del derecho a la protección de datos implica el poder de disposición sobre los datos personales (STC 254/1993, fundamento jurídico 7º), que en ningún caso podrán ser utilizados para una evaluación del titular, quien además tendrá derecho a ser indemnizado por los daños y perjuicios ocasionados como consecuencia del incumplimiento de las normas contenidas en la LOPD, criterio que se hizo firme en la doctrina constitucional española a partir de la Sentencia 292/2000.

6.3.1.- Importancia de la STC 292/2000

La STC 292/2000 marca un cambio decisivo para el derecho a la protección de datos personales, desde el momento en que el Tribunal Constitucional le atribuye a este nuevo instituto la consideración de derecho fundamental autónomo. Luego vendrá la Carta de los Derechos Fundamentales aprobada como Declaración de la Cumbre de Jefes de Estado y de Gobierno de la Unión Europea, celebrada en Niza el 7 de diciembre de 2000 y hoy integrada en el Tratado de Lisboa, en vigor.

La importancia de la STC 292/2000 es la incorporación de un nuevo derecho fundamental en España, y su influencia en toda Europa y en el mundo. En virtud de este nuevo derecho fundamental, toda persona puede decidir sobre sus propios datos. El pronunciamiento también es innovador al separar del derecho a la intimidad la protección de los datos personales, a la cual considera un derecho distinto.

Con respecto a la naturaleza del consentimiento del afectado para el tratamiento de sus datos de carácter personal, el TC consideró que la LOPD, al exigir que en determinados supuestos, y por razón de tratarse de datos especialmente protegidos, el titular del dato debe manifestar su consentimiento en forma expresa (art.7.3) y escrita (art.7.2). De esta forma está admitiendo que en los demás supuestos pueda otorgarse de forma tácita.

Centrándonos en el análisis de la Sentencia debemos decir que el objeto de tutela del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que ya estaría protegida por el artículo 18.1 de la Constitución Española, sino todos los datos de carácter personal.

Efectivamente, el TC viene, en esta Sentencia, a extender este derecho fundamental a todos los datos personales, tanto públicos como privados o íntimos.

Es decir que, al extender la tutela sobre todos los datos personales, está alcanzando a aquellos que identifiquen o permitan la identificación de la persona, y que puedan configurar su perfil ideológico, racial, sexual, económico, etc.

De esta forma, el derecho fundamental a la protección de datos personales se concreta en un poder de disposición y de control sobre los datos personales, que faculta a la persona para decidir cuáles de sus datos va proporcionar a un tercero, sea la Administración o un particular; para decidir cuáles puede este tercero recabar, o para saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Al describir el contenido del derecho a la protección de los datos personales, podemos reunir los poderes de disposición y control de tales datos, en los siguientes: a) facultad de consentir la recogida de los datos; b) facultad de consentir la obtención y acceso a los datos personales; c) facultad de consentir sobre su posterior almacenamiento y tratamiento; d) facultad de consentir el uso de los datos personales, o usos posibles, por un tercero, sea la Administración Pública o un particular.

Es importante remarcar que así configurado este nuevo derecho fundamental, requiere como complementos indispensables, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, así como poder oponerse a esa posesión. Por tanto, cualquier actuación que suponga privar a la persona de aquellas facultades de disposición y control sobre sus datos personales, constituirá un ataque y una vulneración de su derecho fundamental a la protección de datos. En este sentido ya había pronunciamiento del TC en la Sentencia 11/1981, de 8 de abril, en la que expresaba “se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección”.

Concluye el TC en la Sentencia 292/2000 que la LOPD, en los artículos cuestionados judicialmente, es contraria a la Constitución al vulnerar el derecho fundamental a la protección de datos, contenido en el artículo 18.4 CE.

La norma que permita a un poder público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales sin consentimiento del titular de esos datos, sólo estará justificada si, ante circunstancias de grave peligro para la vida o la salud de la población, responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. La ley que debe regular los límites a los derechos constitucionales, debe hacerlo con escrupuloso respeto a su contenido esencial, evitando conculcar el derecho fundamental cuyo contenido quiere regular, situación que se concreta al autorizar a otro poder público para fijar en cada caso las restricciones que pueden imponerse a dicho derecho fundamental. Esta doctrina es la que sustenta el fallo del Tribunal Constitucional, cuando declara nulos y contrarios a la Carta Magna, los preceptos de la LOPD impugnados.

En el caso del artículo 24.1 de la LOPD, la expresión "funciones de control y verificación" provoca incertidumbre por cuanto que entiende debe ser rechazada, y habilita a la Administración para restringir derechos fundamentales, renunciando la propia ley a fijar por sí misma estos límites y transfiriendo esa facultad o poder a la Administración para hacerlo.

Esto mismo es aplicable al empleo que hace el artículo 24.2 de la expresión "interés público", como fundamento de la imposición de los límites. Por otra parte, debemos aclarar que toda la actividad administrativa, en último término, persigue la salvaguardia de intereses generales, cuya consecución constituye la finalidad a la que debe servir con objetividad la Administración (art.103.1 CE). Respecto de la restricción al ejercicio del derecho que supone la "persecución de infracciones administrativas", establecido en el artículo 24.1 de la LOPD, también objeto de recurso por parte del Defensor del Pueblo cuyos argumentos han sido acogidos por el Tribunal, se declara carente de todo fundamento constitucional, pudiendo incluso suponer una práctica que cause grave indefensión en el interesado a la hora de

articular su defensa en la tramitación de un expediente, derivado de la comisión de infracciones administrativas, al no poder rebatir, por ignorarlos, datos que la propia Administración tiene y puede usar en su contra.

La argumentación analizada sustenta también la decisión del Tribunal Constitucional respecto de la nulidad del apartado 2 del artículo 24 LOPD, que venía a establecer la restricción de los derechos de acceso, rectificación y cancelación, en caso de la concurrencia de "intereses de terceros más dignos de protección", por cuanto, en definitiva, conlleva dejar a la decisión administrativa la fijación de límites al ejercicio del derecho fundamental a la protección de los datos de carácter personal.

La STC 292/2000 se edifica sobre el respeto a la vida privada de la persona y de su familia, como elementos constitutivos del límite al acceso de la información que de ella existe almacenada en diversos archivos (de titularidad pública o privada) de modo que el propio almacenamiento y tratamiento de aquella información debe estar sometido a fuertes constricciones, que obligan a una interpretación restrictiva y rigurosa de los términos en los que esa información puede divulgarse o transmitirse.

Con este fundamento el TC desglosa el artículo 18.4 CE de los contornos del artículo 18.1 CE, para centrar la verdadera dimensión de la protección de la privacidad frente al uso incontrolado de la informática. La invocación del artículo 18.4 CE se produce con un claro objetivo, llamado a buscar un anclaje positivo para un nuevo derecho fundamental, que con esta fórmula será ubicado entre los reconocidos por la Constitución. El resultado ha exigido una labor de interpretación verdaderamente flexible, que ha partido de la expansión de los contornos de la intimidad hacia la vida privada.

El TCE extiende el ámbito de la intimidad a la privacidad, al control de los datos personales y a su relación con la libertad individual también amenazada ante las múltiples posibilidades de la informática. El objeto de protección es, en

definitiva, algo ajeno y distinto a la intimidad, aunque en algunas ocasiones se lo solape o incluya dentro de la misma.

De esta manera, el TCE reconoce la existencia de un derecho autónomo, relativo al *habeas data*, en el que se acogen facultades de control de los afectados, enarboladas en torno a la información y al consentimiento en la recogida y cesión de datos personales, así como a las posibilidades de acceso, rectificación y cancelación de ellos.

Llegados a la convicción de la necesidad de proteger una esfera del individuo más amplia que la intimidad, la sentencia fuerza la intelección del artículo 18.4 CE y convierte en pilar básico lo que no deja de ser un simple mandato constitucional para que el legislador limite el uso de la informática. Con esta fórmula hermenéutica, el TC da cobertura a un nuevo derecho fundamental, signo de los tiempos que corren, y que el Alto Tribunal justifica con el mandato dirigido al legislador para establecer la reserva de ley dentro de la función de garantía propia de los derechos fundamentales en el Estado democrático y Social de Derecho.

En esta Sentencia observamos que frente a la función del derecho fundamental a la intimidad del art. 18.1 CE, el TC perfila la singularidad de este derecho a la protección de datos, prolongando su garantía no solo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones el máximo intérprete ha definido, en términos más amplios, como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, profundamente conectada con el respeto a la dignidad personal (STC 170/1987, de 30 de Octubre, fj. 4º), como el derecho al honor, citado expresamente en el art. 18.4 CE e igualmente en expresión bien amplia del propio 18.4 CE, al pleno ejercicio de la persona, para concluir una definición del derecho a la protección de datos de carácter personal como aquel derecho que: "persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado".

6.3.2.- ¿Protección de datos o autodeterminación informativa en la STC 292/2000?

Una vez que el TC ha definido el derecho a la protección de datos personales, cabe preguntarnos por su concepción del derecho a la autodeterminación informativa.

Siguiendo el hilo argumental de la sentencia 292/2000, nos surge la duda sobre la sinonimia entre la autodeterminación informativa y la protección de datos de carácter personal, y nos preguntamos si acaso aquella incorpora algunas nociones distintas al concepto de protección de datos.

En realidad, en el pronunciamiento del TC no se encuentra una distinción de conceptos y puede observarse que en la STC 292/2000 ambas menciones se utilizan indistintamente. Son el Defensor del Pueblo y el Abogado del Estado quienes usan la denominación "autodeterminación informativa"; en cambio, los miembros del TC español usan la terminología "protección de datos de carácter personal", lo cual no es extraño, ya que el Alto Tribunal se encontraba estudiando la constitucionalidad de una Ley Orgánica cuyo objeto y nombre es la protección de los datos de carácter personal.

Distintos autores mencionan a la STC 53/1985 de 11 de abril, como la sentencia en la cual el TCE coloca a la autodeterminación consciente y responsable de la propia vida dentro del concepto de dignidad del ser humano. La dignidad humana garantiza un status jurídico o libertad en un ámbito de la existencia. Se trata de una libertad específica cuyo significado corre a cargo de la identidad del sujeto, con la consiguiente definición de su propia personalidad o conjunto de cualidades que la distinguen del resto de la humanidad. De manera que vida privada y autodeterminación informativa caminan muy cerca por la senda de la identidad.

La autodeterminación informativa hace referencia a la decisión personal e intransferible de determinar qué es lo que cada uno de nosotros quiere que los demás sepan de nuestra persona, posibilidad que alcanza también al derecho a

conocer los datos propios que obran en archivos ajenos y en este punto se relaciona directamente con la protección de los datos de carácter personal, lo que no deriva únicamente en la visión que los demás puedan tener de nuestra persona, sino, yendo más lejos, en la definición de nuestra propia identidad a partir de datos nuestros, que no obstante y por circunstancias de la vida, pudieran ser desconocidos para nosotros.

No es tanto la protección de la vida privada, cuya afinidad con la intimidad es indiscutible a pesar de la mayor amplitud de su concepto, como la protección de nuestro propio ser, de nuestra identidad, de nuestra personalidad. Por ello la protección se dirige a la libertad interna que maneja nuestra conducta externa y que, en definitiva, modela nuestra personalidad desde el ámbito de la vida privada.

De hecho, es fácil suponer que muchos comportamientos humanos se frustrarían si los implicados supieran, o al menos sospecharan, que las informaciones referentes a su persona y a su vida iban a trascender al conocimiento de terceros. De modo que el derecho a la autodeterminación informativa, sin dejar de ser una manifestación de los derechos de la personalidad, es un derecho fundamental derivado de la dignidad.

Y en este terreno, es indiscutible que los datos personales constituyen el conjunto de referencias por el cual el individuo se define, de manera que la conjunción de todos sus datos personales conforman su identidad, con las distintas expresiones de su personalidad. La utilización de aquellos datos implica, además, las libertades inherentes a la dignidad de la persona, desde el ámbito interno del sujeto a decidir su conducta más allá de la opinión pública o de su conocimiento por parte del Estado.

La protección de datos de carácter personal se convierte, entonces, en un instrumento necesario para garantizar a la persona un espacio de protección en el que pueda desarrollar su personalidad individual y social, afirmar su identidad, y

auto-determinarse libremente, ejerciendo un verdadero control sobre su vida privada y sobre su información personal.

De modo que el carácter primordial reside, en realidad, en la autodeterminación informativa, verdadero derecho fundamental que enlaza en la esencia misma de la dignidad humana.

Pareciera ser que tanto la doctrina como la jurisprudencia y las normas han cambiado las denominaciones, pero, en realidad, cuando se habla de protección de datos o lo que es lo mismo, de *habeas data*, hay que entender la referencia a la autodeterminación informativa y viceversa.

A modo de conclusión, podemos resumir que el TC, a través de su jurisprudencia, ha evolucionado desde el derecho a la intimidad como un límite a la informática, a un nuevo y distinto derecho a la libertad informática, entendido como el derecho a la protección de los datos personales y a la autodeterminación informativa.

En este sendero evolutivo el TC ha establecido también al derecho a la protección de los datos personales como un derecho fundamental autónomo, configurando su contenido con los principios y derechos que se contemplan en la Ley Orgánica 15/1999 (LOPD).

De esta forma, además de la regulación general contenida en el artículo 11 de la LOPD, aplicable a las Administraciones Públicas, el artículo 21.1, tras la Sentencia analizada, restringe la posibilidad de la cesión de datos entre las Administraciones Públicas al ejercicio de las mismas competencias o competencias que versen sobre las mismas materias, o al tratamiento posterior con fines históricos, estadísticos o científicos.

Por tanto, y salvo que expresamente venga a hacerlo una norma con rango de Ley, fuera de las excepciones de carácter general del artículo 11.2 LOPD, y específicas del artículo 21.1 y 2 LOPD, será necesaria la autorización de las

personas afectadas por los datos del archivo, para que estos puedan cederse entre las Administraciones públicas.

Por otra parte, el derecho de información al ciudadano, acogido en el artículo 5.1 y 2 LOPD, sólo podrá ser excepcionado por las Administraciones Públicas cuando dicha información pueda afectar a la defensa nacional, a la seguridad pública, o a la persecución de una infracción penal.

Las únicas excepciones específicas alegables por las Administraciones Públicas, frente al ejercicio de los derechos de acceso, rectificación y cancelación realizado por los ciudadanos serán, tras la supresión del apartado 2 del artículo 24, las contempladas en el artículo 23 de la LOPD, referentes a archivos o banco de datos de las Fuerzas y Cuerpos de Seguridad, así como los ficheros de la Hacienda Pública.

Finalmente, cabe destacar que la influencia de la doctrina sentada por el TCE en la STC 292/2000 tiene alcance universal.

7.- Principios de la protección de los datos de carácter personal

Los principios establecidos por la doctrina, en materia de protección de datos de carácter personal, tienen la intención de determinar conceptualmente el modo más eficaz de proteger la intimidad de las personas frente a la evolución de las tecnologías de la información y de las comunicaciones. Se busca proteger a la persona, a los efectos de que ella salvaguarde su libertad, ejerciendo el dominio y el poder de decisión sobre sus datos personales. Observamos que los datos personales son el medio para llegar al fin: la protección integral de la persona. Constituyen un elemento fuerte de toda legislación en la materia, ya que los datos personales son las unidades que aportan información sobre el sujeto. Otro elemento central de toda

legislación de protección de datos personales son los derechos que se le otorgan a la persona[148].

Estos principios, también contemplados por el Convenio 108 del C. de E., son el contenido mínimo que debería estar presente en toda legislación de protección de datos personales, sobre los cuales abundaremos en los capítulos siguientes de esta tesis[149].

Así, diferentes autores especializados en la materia[150] han considerado que toda legislación de protección de datos personales debe exigir:

a) Que los datos acumulados por bancos y usuarios de datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimas para las que se hayan obtenido[151];

b) Como consecuencia del principio anterior, las leyes deben prohibir que los datos personales se usen para finalidades distintas de aquellas para las que fueron recogidos;

c) Deben exigir al titular del banco de datos que los datos almacenados sean exactos y estén en constante actualización;

d) En consecuencia con el punto anterior, si el titular o responsable del banco de datos determina que algún dato no es exacto o está incompleto, debe proceder a su cancelación o sustitución por datos correctos;

e) La Ley debe exigir que los datos almacenados en un banco de datos sean cancelados cuando dejen de ser necesarios o útiles para la función prevista, y en este caso prohibir su conservación, salvo cuando se justifique mantenerlos como valores históricos;

[148] Rebollo Delgado, L.; Serrano Pérez, M. (2008), Op. cit., p. 125.
[149] Consejo de Europa, Convenio 108. Op. cit.
[150] Rebollo Delgado, L. y Serrano Pérez, M. (2008). Op. cit., p. 126.
[151] La LORTAD española contemplaba este principio en el art. 4. La vigente LOPD (Ley Orgánica de Protección de Datos) española y la ley argentina 25.326 de Protección de Datos Personales, también lo expresan en el art. 4. La LOP lo hace en el art. 4 inc. 1°.

f) Debe exigir al banco de datos que el almacenamiento de los datos personales permita al afectado o titular del dato, el ejercicio del derecho de acceso a sus datos personales;

g) Debe prohibir a los bancos de datos recoger datos por medios fraudulentos, desleales o ilícitos;

h) También debe prohibir la creación o conservación de archivos de datos con la finalidad exclusiva de almacenar datos sensibles, es decir, datos que revelen ideología, religión, creencias, origen racial o vida sexual de las personas;

i) Debe exigir a los bancos de datos el consentimiento del afectado cuando los datos recabados sean de contenido sensible, y sólo autorizar a recabar este tipo de datos sin el consentimiento del afectado, cuando sean absolutamente necesarios para los fines de una investigación concreta realizada por las Fuerzas y Cuerpos de Seguridad, o con motivos de prevención de epidemias, etc.;

j) La doctrina aconseja que toda ley de protección de datos personales contenga distintos niveles de protección y dentro de ellos, que contemplen una protección especial para los datos referentes a ideología, religión o creencias[152] y una protección media para los datos que se refieran al origen racial, salud o vida sexual;

k) La doctrina entiende que dentro de la protección especial aconsejada para los datos sensibles, se prohíba que toda persona sea obligada a declarar sobre los datos personales de carácter sensible, salvo que el afectado consienta expresamente y por escrito;

l) Aun en el caso anterior, el banco de datos debe advertir al afectado su derecho a no prestar su consentimiento;

[152] LORTAD: artículos 7 y 8.

ll) El derecho comparado en general ha coincidido en que los datos referentes al origen racial, salud o vida sexual, sólo podrán recabarse cuando lo disponga la ley por razones de interés general, o cuando el afectado consienta expresamente por escrito u otra fórmula probatoria que dé certeza;

m) Los datos relativos a la comisión de infracciones penales o administrativas sólo pueden ser incluidos por el Estado en bancos de datos públicos, de acuerdo con lo normado por una ley del Estado;

n) Para dar mayor seguridad a los datos[153], la doctrina entiende que la legislación de protección de datos debe establecer un responsable de los datos, el cual deberá adoptar las medidas necesarias para mantener la seguridad de los datos, de modo tal que eviten su alteración, pérdida o acceso no autorizado;

ñ) Con idéntico fundamento al manifestado en el punto anterior, la doctrina planteó la necesidad de prohibir el registro de datos en archivos o bancos de datos que no reúnan las condiciones de seguridad que reglamentariamente establezcan los Estados;

o) Todo responsable de un archivo o banco de datos está legalmente obligado a mantener el secreto sobre los datos personales de terceras personas registradas en las bases de datos[154]. El deber de secreto como obligación legal también recae sobre las demás personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal, aun después de haber finalizado la relación con el titular o el responsable del fichero;

p) El tratamiento automatizado de datos personales requerirá consentimiento tácito o presunto del afectado, otorgado en cualquiera de las formas admitidas por el derecho; excepcionalmente, las leyes pueden disponer que el consentimiento sea otorgado en forma expresa. Para que el

[153] LORTAD: artículo 9.
[154] LORTAD: artículo 10.

consentimiento sea considerado válido es necesario que los datos no se recaben por medios fraudulentos, desleales o ilícitos. El derecho a la protección de los datos personales es un derecho personalísimo y por lo tanto el consentimiento puede ser revocado en cualquier momento, sin que sus efectos sean retroactivos;

q) Cuando se tratare de datos relativos a ideología, religión o creencias, para que el consentimiento sea válido, el interesado debe ser advertido sobre su derecho a negarse a prestar el consentimiento;

r) Otro requisito para la validez del consentimiento es que de modo previo e inequívoco se advierta al interesado: de la existencia de un fichero automatizado, la finalidad del mismo, los destinatarios de la información, el carácter obligatorio o facultativo de sus respuestas a las preguntas planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, de la identidad y dirección del responsable del fichero;

s) Cuando se utilicen cuestionarios u otros impresos para la recogida de datos, deberán figurar las advertencias señaladas en los puntos anteriores;

t) Debe preverse el consentimiento del afectado para la cesión de datos; además se requiere que el cesionario sea determinado o determinable, siendo nulo el consentimiento en caso contrario. Serán nulas las cesiones excesivamente amplias, en las que se deje exclusivamente en manos del cedente la decisión de ceder los datos a una u otra persona, y el afectado no pueda saber en último término, mediante reglas sencillas de identificación, quién dispone de sus datos personales;

u) También será nulo el consentimiento cuando no conste la finalidad de la cesión;

v) Puede eximirse del consentimiento al afectado, sólo en casos determinados; por ejemplo, cuando una ley disponga otra cosa; cuando los datos se recojan en fuentes accesibles al público; cuando los datos provengan de archivos de titularidad privada, cuando se refieran a personas vinculadas por una relación comercial, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato; cuando la cesión de los datos tenga por destinatario a los Jueces o Tribunales en el ejercicio de las funciones que tienen atribuidas[155];

w) Tampoco será necesario el consentimiento, cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un archivo automatizado, o realizar los estudios epidemiológicos[156];

8.- Autoridad de control para la protección de los datos

La evolución del derecho a la intimidad y a la protección de los datos de carácter personal pasó por distintas etapas hasta llegar a comprender la necesidad de crear autoridades de control o de aplicación de la legislación en la materia.

Originariamente, las autoridades de control nacieron para dotar a la regulación de servicios públicos de una mayor eficacia y operatividad. El éxito alcanzado en esas áreas regulatorias ha impulsado a las leyes de protección de datos personales a contemplarlas para también obtener una mayor eficacia y operatividad regulatoria en la materia. Actualmente, las legislaciones más avanzadas entienden que es necesaria la presencia de una autoridad de aplicación que velé por el cumplimiento de las normas del sector de los datos personales.

Así nacieron estas nuevas instituciones de control en materia de protección de datos personales, con la finalidad de cumplir el deber que tiene el Estado de garantizar el respeto y la correcta aplicación de la legislación específica y general.

[155] LORTAD: art. 19.
[156] LGSE (España): Ley General de Sanidad Nº 14/1986 de 25 de abril.

En este sentido, el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, ya menciona a estas autoridades reguladoras en su artículo 2º, donde las denomina como "autoridad controladora del fichero", y las define como "la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán"[157]. Posteriormente, también el derecho comunitario europeo se ocupó de las autoridades reguladoras en la Directiva 95/46/CE, en su art. 2º, inciso f), donde las denomina "tercero" y las define como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento".

Los sistemas elegidos por la legislación comparada son diferentes, pero aquellos que optaron por la creación de un organismo de control, también diseñaron formas variadas. El sistema y el perfil del organismo creado al efecto han tomado en algunos casos la forma de una autoridad unipersonal y en otros, la forma de un cuerpo colegiado. En algunos casos se ha buscado independencia del poder ejecutivo, en otros el organismo de control funciona como una dependencia más de ese poder[158].

Las opciones son diferentes: autoridad independiente, autoridad dependiente del Gobierno, autoridad dependiente del parlamento o un control judicial difuso de la aplicación de la ley sin que exista una autoridad de control específica.

Si observamos las diferentes variantes de organismos de control, podemos encontrar:

[157] Consejo de Europa: Convenio 108 (1981). Op. cit., Art. 2º.
[158] Del Peso Navarro, E. *La ley de protección de datos, la nueva LORTAD*. Editorial Díaz de Santos. Madrid, 2000, p. 89.

8.1.- Autoridad de control independiente

Con estas características, podemos encuadrar a la mayoría de los organismos de control creados por la legislación europea. Entre ellos se encuentra, en España, la Agencia de Protección de Datos Personales[159], ente público independiente creado por ley[160], como una variante de autoridad administrativa que a la vez cumple funciones de Comisario o Defensor de los Datos[161].

La anterior ley española de protección de datos personales, hoy ya derogada, conocida por la sigla de LORTAD[162], manifestaba en su exposición de motivos el carácter independiente del órgano y la absoluta independencia de su Director en el ejercicio de sus funciones. Parte de la doctrina española ha polemizado con la independencia de la Agencia de Protección de Datos[163], por considerar que debería ser un órgano inter-poderes, que cuente con una presencia auténticamente independiente, que ejerza una función de fiscalización y defensa de los derechos de los ciudadanos en los aspectos que se pretende proteger. Se critica, también, que no se le hayan asignado en forma clara las competencias e independencia necesarias para su eficaz funcionamiento.

Pero más allá de las críticas, la Agencia de Protección de Datos cuenta con una independencia establecida por la Ley y su Reglamento, establecida en forma concreta, de tal forma que su diseño le ha permitido tener una actuación importante en los últimos años, ganar respeto y reconocimiento de la sociedad española.

---

[159] España. Real Decreto 428/1993, de 26 de marzo, por el cual se regulan las funciones y la actuación de la Agencia de Protección de Datos española.

[160] El artículo 35 primera parte de la LOPD española (Ley Orgánica 15/99), expresa: "La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente ley y en un estatuto propio, que será aprobado por el gobierno".

[161] LOPD, España. Op. cit.: Título VI, artículos 34 al 42.

[162] LORTAD: Ley Orgánica de Regulación del Tratamiento Automatizado de Datos (Ley Orgánica 5/1992, España).

[163] Davara Rodríguez, M. "La Ley española de protección de datos (LORTAD) ¿una limitación del uso de la informática para garantizar la intimidad?" Revista Actualidad Jurídica N° 76. Editorial Aranzadi, Pamplona (España), 12 de noviembre de 1992.

La independencia del organismo, en realidad está muy ligada con la independencia de su Director. En el sistema español, el Director de la Agencia de Protección de Datos es designado por el Gobierno a propuesta del Ministro de Justicia, luego de debatir entre los miembros del Consejo Consultivo[164]. Su mandato dura cuatro años y sólo puede ser removido de su cargo por las causales que prevé el artículo 36 de la LOPD[165]. Las únicas causas establecidas por ley para fundar el cese antes de la expiración del mandato del Director de la Agencia de Protección de Datos, son las siguientes: a) por petición propia; b) por incumplimiento grave de las obligaciones del cargo; c) por incapacidad sobrevenida para el ejercicio de sus funciones; d) por incompatibilidad; y, e) la condena por delito doloso.

El art. 36 de la LOPD española de 1999, en su apartado 2º, expresa textualmente que el Director de la Agencia de Protección de Datos ejercerá sus funciones con plena independencia y objetividad, y no estará sujeto a instrucción alguna en el desempeño de aquellas. En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que este le realice en el ejercicio de sus funciones. El artículo 37 de la misma ley establece como funciones de la Agencia de Protección de Datos, las siguientes: a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos; b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones

[164] El Consejo Consultivo: es un órgano colegiado de asesoramiento del Director de la Agencia de Protección de Datos, emitiendo su informe en todos los asuntos que les someta, pudiendo formular propuestas en temas relacionados con la Agencia. Los miembros del Consejo Consultivo serán nombrados y, en su caso, cesados por el Gobierno. Estos según el artículo 19 del Estatuto, serán propuestos de la siguiente forma: a) El Congreso de los Diputados propondrá, como Vocal, a un Diputado. b) El Senado propondrá como Vocal, a un Senador. c) El Ministro de Justicia propondrá al Vocal de la Administración General del Estado. d) Las Comunidades Autónomas decidirán, mediante acuerdo adoptado por mayoría simple, al Vocal a proponer. e) La federación Española de Municipios y Provincias propondrá al Vocal de la Administración Local. f) La Real Academia de la Historia propondrá, como Vocal, a un miembro de la corporación. g) El consejo de Universidades propondrá a un Vocal experto en la materia de entre los cuerpos docentes de enseñanza superior e investigadores con acreditado conocimiento en el tratamiento automatizado de datos. h) El Consejo de Consumidores y Usuarios propondrá mediante terna, al Vocal de los usuarios y consumidores. i) El Consejo Superior de Cámaras de Comercio, Industria y Navegación propondrá, mediante terna, al Vocal del sector de ficheros privados.

[165] LOPD: Ley Orgánica de Protección de Datos (L.O. 15/99, España).

reglamentarias; c) Dictar, en su caso y sin perjuicio de las competencias de otros órganos las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la presente Ley; d) Atender las peticiones y reclamaciones formuladas por las personas afectadas; e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de datos de carácter personal; f) Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros cuando no se ajusten a las disposiciones de la presente Ley; g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley; h) informar, con carácter receptivo, los proyectos de disposiciones generales que desarrollen esta Ley.; i) Recabar de los responsables de los ficheros cuanta ayuda e información se estime necesaria para el desempeño de sus funciones; j) velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine; k) Redactar una memoria anual y remitirla al Ministerio de Justicia; l) ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos. Así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales; ll) velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto de la recogida de datos estadísticos y el secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46; m) cuantas otras le sean atribuida por normas legales o reglamentarias.

En este caso, y para cumplir con estas funciones asignadas por la ley, la Agencia de Protección de Datos española fue dotada con potestad reguladora, instructora, inspectora, sancionadora e inmovilizadora:

a) Potestad reguladora: El artículo 5 del Estatuto establece que la Agencia colaborará con los órganos competentes en el desarrollo normativo

así como en la aplicación de la Ley. No tiene una potestad reglamentaria, pero sí de cooperación en el desarrollo de la normativa:

b) Potestad instructora: Esta facultad permite instruir expedientes que correspondan para sancionar las infracciones cometidas.

c) Potestad inspectora: Según el artículo 40 de la LOPD, corresponde a la Agencia de protección de Datos la inspección de los bancos de datos o archivos comprendidos en la Ley. Correspondiendo dicha función, según el artículo 27 del Estatuto, a la Inspección de Datos.

d) Potestad sancionadora.: El órgano de control debe ejercer dicha función en los términos por la ley de protección de datos personales. En la legislación española, esta potestad se otorga a la Agencia de Protección de datos personales, prevista en el Título VII de la Ley, y en este sentido, el artículo 45 de la misma norma otorga al Director de la Agencia de Protección de Datos la función de iniciar, impulsar la institución y resolver los expedientes sancionados referentes a los responsables de los ficheros privados. La ley española manifiesta que contra estas resoluciones procede el recurso contencioso-administrativo.

e) Potestad inmovilizadora: esta potestad tiene relación con la inmovilización de los archivos o bases de datos. En este sentido, la ley española contempla la potestad inmovilizadora en el art. 49 de la LOPD. El Director de la Agencia puede, mediante resolución motivada, inmovilizar los archivos automatizados.

En los distintos sistemas estudiados, encontramos que la legislación española tributaria del derecho comunitario europeo y, por lo tanto, similar al resto de la legislación de los Estados miembros de la Unión Europea, ha elegido la creación de una autoridad de aplicación y control autónoma e independiente del Poder Ejecutivo. La autoridad de control española ha mostrado buenos resultados en el cumplimiento de sus funciones, incluso en el ejercicio de la potestad sancionadora.

En su sitio web y en las memorias puede apreciarse una gran cantidad de sanciones aplicadas, incluso algunas muy graves.

8.2.- Autoridad de control dependiente del Poder Ejecutivo

La legislación también puede optar por crear una autoridad dependiente del Gobierno. Este es el caso de la legislación Argentina Nº 25.326, por la cual se crea un órgano de control estatal que tiene como misión velar por el cumplimiento de la ley y llevar el control de todos los bancos de datos existentes, para determinar quiénes comercializan información personal y fiscalizar que tipos de datos se almacenan; podrá también verificar de dónde se saca la información. Las personas pueden denunciar los casos de incumplimientos de la ley que les afecten, ante el órgano de control, que debe entrar en acción, inhabilitando, suspendiendo, aplicando multas e incluso prohibiendo a una empresa que siga prestado este servicio.

Esta ley crea un organismo de control, ente oficial de aplicación que depende del Ministerio de Justicia de la Nación. Tiene entre sus principales funciones el registro de empresas, organismos y particulares que trabajen con bases de datos personales y confidenciales. Cada empresa debe contar con un permiso otorgado por el órgano de control, que la habilite a trabajar. El órgano de control puede aplicar sanciones a aquellas empresas que violen la ley, mediante multas, suspensiones e inhabilitaciones

La ley determina que el órgano de control sea dirigido por un Director, designado[166] por el Poder Ejecutivo por el término de 4 años.

La ley de protección de datos personales argentina también habilita la posibilidad de que las asociaciones o entidades representativas de responsables o

[166] El proyecto de ley aprobado por el Congreso de la Nación (Argentina) establecía que el Ejecutivo designaría al Director de la Agencia con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia. Esta parte del artículo fue vetada por el Poder Ejecutivo, quitándole todo aspecto de independiente al organismo de control.

usuarios de bancos de datos de titularidad privada, propongan una autorregulación o código de conducta para el tratamiento de datos personales en función de los principios establecidos en la ley, que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información. La ley establece que el órgano de control será el responsable de llevar un registro de estos códigos de conducta.

También establece sanciones administrativas y penales para los responsables o usuarios de bancos de datos. Las sanciones administrativas son aplicadas por la autoridad de control, y pueden contener un apercibimiento, suspensión, o una multa que se gradúa entre mil pesos y cien mil pesos. Las sanciones también pueden contener la clausura o cancelación del archivo, registro o banco de datos[167].

Aun cuando el parlamento argentino diseñó un ente de control independiente, el Poder Ejecutivo vetó los artículos de la ley 25326 que establecían esa independencia, transformando a la autoridad de aplicación en un mero apéndice del Poder Ejecutivo.

Los organismos de control diseñados en el derecho comparado para controlar las empresas concesionarias de servicios públicos han tenido en general una deficiente actuación. Por eso, la doctrina aconseja organizar entes reguladores independientes del Estado. Esta solución ha encontrado una gran resistencia política; sin embargo, los entes reguladores dependientes del Estado han demostrado una gran ineficacia e incapacidad para cumplir con sus fines. Más aun, en Latinoamérica, en muchos casos, sólo fueron usados por el poder político como una fuente de empleo a distribuir entre su clientela electoral o más grave, como cajas receptoras de sobornos prevenientes de las empresas concesionarias.

Por este motivo, en general, la doctrina aconseja que los organismos de control sean autónomos, públicos pero no estatales, directamente fiscalizados por el Parlamento y sin ninguna dependencia del Poder Ejecutivo.

[167] Argentina: Ley Nacional Nº 25.326 (promulgada en noviembre de 2000): Artículos 30 y 31.

La autoridad de aplicación y control argentina carece de independencia y autonomía del gobierno central. En la práctica esta autoridad llamada Dirección Nacional de Protección de Datos, no ha logrado proteger a las personas en su derecho a la autodeterminación informativa, tampoco ha realizado una difusión importante sobre el derecho que tiene cada habitante a proteger sus datos personales. Prueba de ello es la escasa cantidad de sanciones muy leves que muestra en su página web: sólo veintidós sanciones leves desde el año 2005 a la fecha.

8.3.- Sistema de control judicial de aplicación de la ley

Otro sistema de control posible es a través del Poder Judicial. Es decir, delegar el control a los jueces, para que velen por el cumplimiento de la ley. Este modelo es el seguido por la legislación chilena, a partir de su ley 19.628 de septiembre de 1999, sobre protección de la vida privada. La ley chilena no crea una autoridad especial y deja que sean los jueces los que ejerzan el control de la aplicación de la Ley, sistema está fortalecido por un control cruzado que realiza el Servicio de Registro Civil e Identificación de las personas, sobre los organismos públicos.

En la práctica este sistema también ha mostrado ineficacia. A primera vista, organizar un sistema de control sobre la protección de los datos de carácter personal a realizarse por medio de la entidad que más datos almacena sobre las personas, en todo el país, no parece lógico. Implica una confusión de roles, ya que pone a controlar a quien debería ser el controlado: el Registro Civil.

Al igual que Chile, EEUU también sigue un sistema de control judicial sobre el cumplimiento de la legislación sobre protección de datos personales, que en el caso de los organismos públicos, se fortalece con un control cruzado, que realiza en el caso de Chile, el Registro Civil e Identificación de las personas[168].

[168] LPDVPCH: Ley chilena sobre Protección de la Vida Privada Nº 19628, en sus artículos 16º y 22º.

8.4.- El encargado de protección los datos

La Directiva europea 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en su art. 18.2 establece que el responsable del tratamiento de los datos personales de una base de datos puede designar un encargado de protección de datos personales con las siguientes funciones: a) hacer aplicar en el ámbito interno, de manera independiente, las disposiciones adoptadas en virtud de la directiva; b) llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información requerida por el apartado 2 del artículo 21 de la directiva, garantizando que el tratamiento de los datos no ocasione una merma en los derechos y libertades de los afectados.

El encargado de la protección de los datos personales[169], conocido en el derecho inglés como *Data Protection Officer*, es una figura que ha sido transpuesta de la directiva 95/46/CE, a sólo algunas legislaciones europeas: Alemania, Francia y Eslovaquia, entre otras. Se configura como una persona física o jurídica en el ámbito interno de una organización -sea ésta pública o privada- y tiene como función principal la aplicación independiente de la normativa sobre protección de datos de carácter personal.

La designación del encargado de la protección de los datos de carácter personal permite la simplificación o la omisión del deber de notificación a la autoridad de control sobre los archivos o tratamientos llevados a cabo. En la práctica, esta figura ha demostrado que su actuación mejora el cumplimiento interno de la legislación en la materia, tanto en el aspecto jurídico, como en el técnico y en el organizativo[170].

[169] Santamaría Ramos, F. *El encargado independiente. Figura clave para un nuevo derecho de protección de datos*. Editorial la Ley. Madrid, 2011; p. 41.
[170] Suñé Llinás, E. y Santamaría Ramos, F. (2010). Op. Cit., p. 2025.

España y Argentina no contemplan en su derecho interno la figura del encargado de la protección de datos de carácter personal, por este motivo, de *lege ferenda,* proponemos la incorporación del encargado de la protección de datos personales, tanto en la legislación de Argentina como en la de España.

9.- Datos personales y telecomunicaciones

En estos tiempos, las empresas de telecomunicaciones se encuentran en plena expansión y crecimiento. Y producto de este fenómeno, su crecimiento empresarial está directamente relacionado con la cantidad de datos personales que recolectan. El Consejo de Europa ya manifestó su preocupación en febrero de 1995, a través de la Recomendación R (95) 4, sobre la protección de los datos de carácter personal en el ámbito de los servicios de telecomunicaciones. Esta recomendación tenía como principal objeto a los servicios telefónicos.

Dos años más tarde, la Unión Europea reguló el tratamiento de los datos personales y la protección de la intimidad en el sector de las telecomunicaciones, mediante la Directiva 97/66/CE del Parlamento Europeo y del Consejo de Europa, del 15 de diciembre de 1997, que vino a complementar la Directiva 95/46/CE, también dictada por el Parlamento y el Consejo Europeo en octubre de 1995, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, con el propósito de dar soluciones a los problemas específicos que plantea el sector de las telecomunicaciones[171].

La Recomendación R (95) 4 del Consejo de Europa, se refiere en sus puntos 3, 4 y 5 a la recolección y el tratamiento de los datos personales. Exige la aplicación del principio de información del usuario y de la comunicación restringida de los datos personales a terceros. La mencionada norma se basa en el principio de consentimiento y otorga los derechos de acceso y rectificación a los titulares de los datos. En este punto la Recomendación permite obviar el consentimiento para la

[171] Artículo 1.2 de la Directiva 97/66.

cesión de datos de carácter personal, cuando se produzca entre operadores de red y proveedores de servicio y sea necesaria para fines operativos y de facturación.

La Directiva 97/66/CE diferencia el derecho de las redes de telecomunicaciones del derecho que regula los contenidos que circulan por ellas. El artículo 2°, inciso d) de la mencionada Directiva, excluye a la radiodifusión sonora y a la televisión del concepto de servicio de telecomunicación[172]. Sin embargo, esta norma legisla sobre los servicios de guía telefónica, del tráfico, de facturación, la seguridad y confidencialidad de los datos, entre otros.

A los efectos de la transposición de la Directiva 97/66 en España, el Real Decreto 1736/1998 aprobó el Reglamento que desarrolla el Título III de la Ley General de Telecomunicaciones, que incluye en su Título V la protección de los datos personales en la prestación de los servicios de telecomunicaciones. Esta norma regula, entre otros temas, los siguientes:

a) Datos personales que pueden ser tratados a los efectos del tráfico y la facturación: el artículo 65 del Real Decreto 1736/1998 enuncia, con carácter limitativo, los siguientes datos personales que pueden ser tratados, a los efectos de facturación y pago de interconexiones: 1) *El número o la identificación del abonado. 2) La dirección del abonado y el tipo de equipo terminal empleado para las llamadas. 3) El número total de unidades que deben facturarse durante el ejercicio contable. 4) El número del abonado que recibe la llamada. 5) El tipo, la hora de comienzo y la duración de las llamadas realizadas o el volumen de datos transmitidos. 6) La fecha de la llamada o el servicio. 7) Otros datos relativos a los pagos, tales como pago anticipado, pagos a plazos, desconexión y notificaciones de recibos pendientes.*

Estos datos sólo se pueden almacenar durante el plazo en el cual la factura es impugnable o exigible el pago de la misma. Una vez vencidos tales plazos, los datos

[172] Suñé Llinás, E. (1999): "La protección de la intimidad en el sector de las telecomunicaciones". Comunicación publicada en las *Actas del XII encuentro sobre Informática y Derecho 98/99*; (obra coordinada por Miguel Ángel Davara Rodríguez). Editorial Aranzadi. Pamplona, 1999, p. 79.

deben ser destruidos o cancelados. Otra opción no prevista por la ley es la posibilidad de bloquear tales datos supuestamente tasados o reglados[173].

Esta misma norma no permite el tratamiento que los operadores de servicios de telecomunicaciones hagan de los datos indicados para la promoción de los propios productos, permitido por la Directiva 97/66. El Real Decreto 1736/1998, añade el requisito del consentimiento previo del afectado, que puede ser expreso o presunto, si no responde a la solicitud del correspondiente operador.

El artículo 66 del Real Decreto establece límites a la facturación detallada para proteger el anonimato de los usuarios del servicio de telefonía, y remite la cuestión, prácticamente en su integridad, a la regulación que se produzca mediante Resolución del Secretario General de Comunicaciones.

Sobre los datos personales incluidos en las guías de abonados al servicio telefónico, el Reglamento reitera la vigencia del derecho de exclusión de tales datos en la publicación de la guía, que puede ejercitar el afectado. El artículo 67 de esta norma, no aclara suficientemente que dichas guías pueden ser impresas o electrónicas para evitar que ante la publicación en exceso de datos, quede de manifiesto que tales datos han de ser los estrictamente necesarios para identificar a un abonado concreto. La inclusión de más datos, en la guía telefónica, requiere siempre el consentimiento del abonado, que además ha de ser expreso.

El Reglamento prevé la posibilidad de que, a petición del abonado, conste en la guía una indicación de que los datos personales no pueden utilizarse para fines de venta directa, y agrega que el ejercicio de estos derechos tiene carácter gratuito[174].

El Reglamento español[175], en su artículo 68, denomina a estas comunicaciones "llamadas no solicitadas para fines de venta directa"; entre ellas incluye a las llamadas completamente automatizadas, de voz o de fax, las cuales

[173] Ibidem. Op. cit., p. 88.
[174] Aparte de reiterar la vigencia del derecho de exclusión, que ya podía ejercitar el afectado,
[175] Real Decreto 1736/1998 (España).

requieren del consentimiento previo del afectado. En este caso el Real Decreto se limita a transponer la directiva en sus estrictos términos.

Los operadores de servicios de telecomunicaciones tienen la obligación de informar a los usuarios sobre el servicio que posibilita identificar la línea llamante y la línea conectada. La identificación de la línea llamante es una prestación que permite que el usuario que recibe la llamada, obtenga información del número telefónico de la línea desde donde se originó la llamada. La identificación de la línea conectada es la prestación que permite que el usuario que origina la llamada obtenga información del número telefónico de la línea a la que haya sido eventualmente conectada su llamada. Sobre estos servicios de identificación de línea llamante y línea conectada, los operadores de servicios telefónicos están obligados a darles a sus abonados las siguientes opciones[176]:

a) Que el usuario que origine la llamada pueda suprimir en cada una de ellas y mediante un procedimiento sencillo y gratuito, la identificación de la línea llamante.

No obstante, se impone eliminar las marcas de supresión en origen de la identificación de la línea llamante, cuando el destino de las llamadas corresponda a entidades autorizadas para la atención de las de urgencia, así como en supuestos de llamadas maliciosas o molestas, de acuerdo con lo establecido en la normativa vigente en cada momento sobre protección y suspensión de las garantías del secreto de las comunicaciones.

b) El abonado que recibe la llamada deberá tener la posibilidad, mediante un procedimiento sencillo, de rechazar las entradas procedentes de usuarios o abonados que hayan suprimido la presentación de la identificación de la línea llamante.

[176] Suñé Llinás, E. Op. cit., p. 89.

c) El abonado que recibe la llamada deberá tener la posibilidad, mediante un procedimiento sencillo y gratuito, de suprimir la presentación a la parte llamante de la identidad de la línea conectada.

Según el artículo 80 del Reglamento[177], los operadores están obligados a ofrecer, a todos los abonados, un procedimiento sencillo y gratuito que permita la posibilidad de poner fin al desvío automático de llamadas a su terminal por parte de un tercero.

Hay autores que piensan que los aspectos estrictamente técnicos sobre la protección de la intimidad en materia de telecomunicaciones, puedan establecerse por medio de los Reglamentos que desarrollen la legislación general de telecomunicaciones de cada Estado europeo (en España, por ejemplo, la Ley General de Telecomunicaciones). Sin embargo, los aspectos más sustantivos de la transposición de la Directiva 97/66 se refieren directamente a los propios derechos fundamentales y, por lo tanto, requieren ser integrados en la ley superior que desarrolle los fundamentos constitucionales de la protección de la intimidad y de los datos de carácter personal[178].

[177] Real Decreto 1736/1998. Op. cit. (España).
[178] Suñé Llinás, E. Op. cit., p. 89.

CAPÍTULO II: PROTECCIÓN DE DATOS EN ESPAÑA Y EUROPA

1.- El Consejo de Europa

1.1.- Las Resoluciones (73) 22 y (74) 29 del Comité de Ministros

Formalmente, podemos considerar a las Resoluciones (73) 22 y (74) 29 del Comité de Ministros del Consejo de Europa como el punto de partida del estudio de una situación que fue altamente demorada por los legisladores; no obstante, es conveniente señalar que los principios y derechos que se recogían en aquellos escritos siguen teniendo vigencia y plena actualidad hoy en día, aunque, como es lógico, adecuados y adaptados a la evolución social y tecnológica.

Los principios que en aquellas recomendaciones se aconsejaban a los Gobiernos de los Estados miembros para que los hicieran respetar en sus territorios, hoy, con pequeñas adaptaciones propias de la evolución tecnológica y de la adecuación práctica e interpretación de las modernas leyes de protección de datos, están vigentes en su totalidad.

A modo de ejemplo, el Comité de Ministros del Consejo de Europa recomendó a los Gobiernos de sus estados miembros, respecto de la creación de bancos de datos, tanto en el sector público como en el privado, tener en cuenta determinados aspectos, cuya finalidad era tomar precauciones contra todo abuso o mal empleo de la información; pueden ser resumidos de la siguiente forma:

1. La información debe ser exacta, mantenida al día, apropiada para el fin para el que fue almacenada y obtenida por medios legales.

2. Todo ciudadano tiene derecho a conocer la información almacenada sobre sí mismo.

3. Las personas que deban operar sobre las bases de datos tienen que estar bajo normas severas de conducta para el mantenimiento del secreto y para prevenir el mal uso de los datos.

4. La seguridad debe ser extremada al máximo para impedir el acceso a las bases de datos a personas no autorizadas o para evitar el desvío de la información, mal intencionadamente o no, hacia sitios no previstos.

5. Si la información va a ser utilizada con fines estadísticos, se revelará de tal forma que sea totalmente imposible relacionarla con ninguna persona en particular.

Casi coincidiendo en el tiempo, veía luz en los Estados Unidos, la llamada Ley de Privacidad[179] que, en su Exposición de Motivos, decía que:

"El Congreso estima que la privacidad de un individuo es afectada directamente por la captación, conservación, uso y difusión de información personal por entes y órganos federales. El creciente uso de ordenadores y de una tecnología compleja de la información, si bien es esencial para el eficiente funcionamiento de las Administraciones Públicas, ha aumentado grandemente el detrimento que para la privacidad individual puede derivarse de cualquier captación, conservación, uso y difusión de información personal[180]".

1.2.- El Convenio 108 del Consejo de Europa

Como ya se dijo, la preocupación europea por un derecho que se ocupe del uso de las telecomunicaciones estuvo presente desde fines de la década de 1960. En la década del 70 se comenzó a debatir sobre la necesidad de una legislación que unificara pretensiones y especialmente que ofreciera un conjunto de medios de

[179] La llamada "ley de Privacidad" de los Estados Unidos data del 31 de diciembre de 1974, aunque en la actualidad y debido a la dinámica y flexibilidad que las nuevas tecnologías de la información imponen a la sociedad, ha sido ya modificada en varias ocasiones.

[180] Cfr. Documentación Informática N° 4. Serie verde. Legislación del Ministerio para las Administraciones Públicas. Dirección General de Organización, Puestos de Trabajo e Informática. Madrid. 1988, pág. 162.

protección a derechos y libertades fundamentales, ante la creciente evolución de las nuevas tecnologías de la información y de las telecomunicaciones. Las instituciones supranacionales europeas no estuvieron ausentes en este debate, del cual surgieron con el tiempo legislaciones sobre el tema. Cierto es que la legislación genérica de la Unión Europea es una legislación de mínimo; sin embargo, en materia de protección de datos, permitió que los Estados miembros fueran elevando progresivamente su nivel de protección, y de esta forma fue generando un efecto homogeneizador en el sistema de tutela eficaz de estos derechos[181].

Esta preocupación de las organizaciones supranacionales europeas en la protección de los derechos de la personalidad y en función de las lesiones que los efectos de la tecnología pueden producir en la sociedad, se formalizó en el Convenio Nº 108 del Consejo de Europa sobre la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, aprobado en 1981 y ratificado por España en 1984. El Consejo de Europa es considerado el promotor de la tendencia legislativa en materia de protección de datos, superadora de los criterios que existían hasta ese momento, los cuales fueron luego receptados por muchas leyes y por algunas constituciones europeas.

El Convenio 108 fue pionero en materia de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales. Ciertamente, su contenido no es derecho directamente aplicable, ya que está compuesto por pautas a las que deben acomodarse las legislaciones internas de países que lo han ratificado. Su texto establece una serie de principios básicos para la protección de datos, señala criterios que regulan su flujo y crea un Comité Consultivo, a quien se encomienda la formulación de propuestas para mejorar la aplicación del Convenio. Este Tratado internacional es un convenio de mínimos, ya que consta de nociones básicas pero fundamentales. Exige que los datos sean obtenidos y procesados lícitamente, que se registren sobre la base de finalidades legítimas y que no sean utilizados de modo incompatible con esos fines. Promueve que los datos tratados sean exactos, puestos

[181] Rebollo Delgado, L. y Serrano Pérez, M. (2008). Op. cit., p. 41.

al día, adecuados, pertinentes y no excesivos. Recoge disposiciones acerca de los datos sensib1es, medidas de seguridad y mecanismos de cooperación internacional. Exige a las leyes nacionales que lo desarrollen, que lo apliquen en razón del territorio, independientemente de la nacionalidad de los afectados (principio de territorialidad) con el propósito de proteger a los extranjeros, en igual alcance que a los nacionales de cada país. Uno de los documentos más importantes en materia de protección de datos personales que ha surgido en Europa fue el Convenio (108) del Consejo de Europa para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal[182], firmado en 1981 en Estrasburgo. Su importancia, además, radica en el compromiso que generó en los Estados firmantes, de dictar en su derecho interno normas de protección de datos personales que respeten el contenido mínimo que exigía el Convenio después de la ratificación[183]. En este sentido, el artículo 4º del Convenio 108, prescribe: "1º Cada Parte adoptará en su derecho interno las medidas necesarias para dar cumplimiento a los principios fundamentales de protección de datos anunciados en el presente capítulo. 2º Tales medidas deberán ser adoptadas lo más tarde en el momento en que el presente Convenio entrare en vigor con respecto a la Parte."

Las disposiciones contenidas en el Convenio 108 buscaron garantizar en el territorio de cada país firmante, a cualquier persona física, el derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal[184]. Cuenta con tres apartados referidos a las consideraciones generales, a los principios, garantías, sanciones y al procedimiento.

El artículo segundo del Convenio establece definiciones con la finalidad de centrar los conceptos sobre los que gira la normativa marco. Es importante destacar que estas definiciones fueron fuente para la Directiva 95/46/CE del Parlamento

[182] Publicado en el BOE (Boletín Oficial del Estado español) número 274, de 15 de noviembre de 1985.

[183] Herrán Ortiz, A.(1998). Op. cit., p. 193.

[184] Artículo 1º del Convenio 108 del Consejo de Europa para la protección de las personas con relación al tratamiento de los datos de carácter personal.

Europeo y del Consejo[185]. Su influencia llegó a la LORTAD y a la LOPD, y desde la legislación española incluso se trasladó a la ley argentina 25.326 de Protección de Datos Personales[186] que en su artículo 2º sigue esta técnica legislativa con similares definiciones. Entre estos conceptos se destacan los siguientes:

Datos de carácter personal: cualquier información relativa a una persona física identificada o identificable[187].

Fichero[188] automatizado: cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado.

Tratamiento automatizado: las operaciones de registros de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados.

Autoridad controladora del fichero: es la persona física o jurídica, que en calidad de autoridad pública actúa como órgano de control sobre el servicio o cualquier otro organismo que sea competente para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deben registrarse y cuáles operaciones se les aplicarán. En España cumple esa función la Agencia Española de Protección de Datos[189] y en Argentina, la Dirección Nacional de Protección de Datos Personales[190]. Aun cuando más adelante analizaremos cada una de estas autoridades de control, podemos adelantar que, al compararlas, encontramos que la autoridad española funciona con una amplia autonomía y

[185] Directiva 95/46/CE, de 24 de Octubre de 1995 (Unión Europea).
[186] Quiroga Lavié, H. (2001). Op. cit., p. 19.
[187] El artículo 2º de la Directiva 95/46/CE (Unión Europea) sigue esta línea conceptual, expresando que datos personales es toda información sobre una persona física identificada o identificable (el interesado); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;
[188] La legislación española también usa el término fichero, mientras la legislación argentina prefirió la palabra archivo.
[189] https://www.agpd.es (último ingreso el 22/07/11)
[190] www.jus.gov.ar/dnpdp (último ingreso el 22/07/11)

autarquía, mientras la autoridad controladora argentina carece de estas importantes características.

Siguiendo con el Convenio (108) del Consejo de Europa, encontramos que distingue entre archivos de titularidad pública y archivos de titularidad privada, indicando en el artículo 3º, que se aplica tanto a los sectores públicos como privados y que cada Estado integrante del Convenio tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos[191], dejando a cada Estado Miembro la posibilidad de conceder a los afectados una protección más extensa que la prevista en el Convenio (art. 11º).

Los principios básicos establecidos por este convenio son los siguientes: a) Calidad de los datos. b) Obtención y tratamiento leal y legal de los datos. c) Los datos se registrarán para finalidades determinadas y legítimas. d) Los datos serán adecuados, pertinentes y no excesivos en relación con las finalidades que se recabaron y registraron. e) Los datos serán exactos y puestos al día.

El Convenio establece unas categorías particulares para aquellos datos que tienen un mayor grado de sensibilidad que otros datos[192]. Sobre estos datos establece una prohibición de tratamiento automático, a menos que el derecho interno prevea las garantías apropiadas. Estas categorías particulares de datos son aquellos relativos al origen racial, las opiniones políticas, las convicciones religiosas u otras creencias, la salud, la vida sexual y las condenas penales.

Con respecto a la seguridad de los datos, el Convenio 108 establece la necesidad de tomar medidas de seguridad contra la destrucción o la pérdida accidental, el acceso, la modificación o la difusión sin autorización.

[191] Artículo 4º del Convenio 108 del Consejo de Europa para la protección de las personas con relación al tratamiento de los datos de carácter personal.
[192] La legislación española y argentina los denomina datos sensibles.

Este acuerdo también establece en el artículo 8º, como garantías complementarias para las personas[193], el derecho de información, acceso, rectificación y borrado, así como el derecho de disposición de un recurso consistente en el derecho de la persona a poder:

a) Conocer la existencia del fichero, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero.

b) Obtener en intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de los datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible.

c) Obtener, en su caso, la rectificación o el borrado de los datos cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos de calidad de los datos.

El Convenio también definitiva que será posible el establecimiento de excepciones cuando, previstas en una ley, constituyan una medida necesaria para la protección de la seguridad del Estado, de la seguridad pública, de los intereses monetarios del Estado, de la represión de infracciones penales, o para la protección de la persona y de los derechos y libertades individuales.

Mediante ley, el convenio indica que se podrán prever restricciones en el ejercicio de los derechos de las personas concernidas cuando se trate de archivos automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, siempre que no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas.

[193] Martín-Casallo López J. (Coord.) *El Consejo de Europa y la Protección de Datos Personales*. Editada por la Agencia de Protección de Datos. Editorial De Arellano. Madrid, 1997, p. 19.

En materia de sanciones, el artículo 10º prevé la posibilidad de establecer sanciones y recursos, e indica que cada Estado Miembro se compromete a establecer las correspondientes sanciones contra las referidas infracciones.

Este acuerdo contempla, en su artículo 13º, un procedimiento entre los Estados signatarios, de cooperación y asistencia en el cumplimiento del Convenio, a cuyo fin se designarán una o más autoridades.

A partir del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, el Consejo de Europa fue dictando, en forma constante e ininterrumpida, copiosas recomendaciones y resoluciones relativas a la protección de los datos personales, que son fuente normativa y doctrinaria en toda Europa y América.

Es importante destacar que el artículo 23 del Convenio 108[194] permite incorporar a Estados no miembros del Consejo de Europa. Esta apertura es, en opinión de Emilio Suñé Llinás, de gran utilidad para aquellos Estados latinoamericanos que no cuenten con legislación sobre protección de datos personales.

El contenido del Convenio 108 fue desarrollado, ampliado y precisado considerablemente por la Directiva 95/46/CE del parlamento europeo y del consejo de 24 de Octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, y se ocupa de armonizar en Europa la legislación en materia de protección de datos. El objetivo de esta Directiva europea aún no ha sido cumplido en su totalidad, dado que deja un amplio margen a los Estados miembros para que transpongan sus disposiciones. Esto ha provocado grandes diferencias en la legislación de los

[194] El artículo 23 del Convenio 108 del Consejo de Europa establece que después de la entrada en vigor del presente convenio, el Comité de Ministros del Consejo de Europa podrá invitar a cualquier Estado no miembro del Consejo de Europa a que se adhiera al Convenio, mediante un acuerdo adoptado por la mayoría.

distintos Estados miembros de la UE; a modo de ejemplo, podemos mencionar el régimen sancionador[195].

2.- Antecedentes en el derecho europeo

En el derecho europeo podemos encontrar que ya a mediados de la década de 1960 se procura alcanzar una legislación de protección a los derechos y libertades fundamentales ante el desarrollo de las telecomunicaciones[196].

Se torna muy complejo el trabajo de traer a estudio todos aquellos antecedentes relacionados con la protección de datos o en forma genérica con la informática y las telecomunicaciones. Por este motivo mencionamos sólo a los que consideramos más importantes. Así, podemos tomar como un primer antecedente en materia de protección de datos personales a la Conferencia de Juristas Nórdicos, celebrada en Estocolmo en mayo de 1967. Esta reunión científica tomó como referencia inmediata anteriores textos internacionales, tales como la Declaración Universal de los Derechos del Hombre, el Pacto Internacional sobre Derechos Civiles y Políticos, así como la Convención Europea sobre los Derechos del Hombre y viene a representar un precedente importante, al reconocer que el derecho a la vida privada es el derecho de una persona a ser dejada en paz, para vivir su propia vida con el mínimo de injerencias exteriores. El alcance internacional de esta reunión de juristas es innegable, dado que acuden a ella representantes de once países, además de los pertenecientes a los países nórdicos, y observadores de varias organizaciones nacionales e internacionales[197].

En otras partes del mundo se realizaron también reuniones científicas de gran importancia en el tema, ya mencionadas en el capítulo I de esta tesis, tales como la Conferencia Internacional de los Derechos del Hombre celebrada en 1968 en Teherán, la cual, a pesar de no desarrollarse en Europa, influye en el derecho europeo, dado que recomienda a la ONU que proceda al estudio de las cuestiones

[195] Suñé Llinás, E. y Santamaría Ramos, F. (2010). Op. cit., p. 2016.
[196] Rebollo Delgado, L.; Serrano Pérez, M. (2008).Op. cit., p. 41.
[197] Herrán Ortiz, A. (1998). Op. cit., p. 55.

planteadas con relación a los derechos del hombre que resulten afectados por el desarrollo de la técnica y la ciencia. En consecuencia, el 19 de diciembre de 1968 la ONU adopta la Resolución 2450, en la que se establece la necesidad de fijar límites a las aplicaciones de la electrónica por su injerencia en los derechos de la persona y solicita al Secretario General que prepare un informe, donde consten resumidamente los estudios realizados, o en curso, sobre la incidencia de las nuevas tecnologías en los derechos humanos. Se inicia así un período de intensos trabajos sobre la problemática que plantea el alcance de los progresos científicos y tecnológicos en los derechos de la persona, que concluye en 1983, con la aprobación por la Comisión de Derechos Humanos de un informe relativo al estudio de los principios rectores pertinentes, respecto de la utilización de los archivos informatizados de datos de carácter personal[198].

Siguiendo este proceso evolutivo, el 23 de enero de 1970 la Resolución 428 de la Asamblea Consultiva del Consejo de Europa se refiere a la intimidad como objeto de obligada protección, frente a la intromisión de la tecnología informática.

Es importante el antecedente mencionado, ya que en 1970 también se aprueba en Costa Rica la Convención Americana sobre Derechos Humanos, en la que nada se declara con respecto a los peligros que acosan a la humanidad, procedentes de la abusiva utilización de las modernas tecnologías de la información.

Sin embargo, en defensa de la persona y del libre ejercicio de sus derechos frente al progresivo desarrollo de los medios informáticos de tratamiento de la información, pronto resultan ineficaces los instrumentos jurídicos de defensa que hasta ese momento le son reconocidos con carácter general al individuo. Es decir, que los medios de defensa y prevención de injerencias en la intimidad y en la vida privada no serán suficientes para la protección de la persona frente a las intromisiones que procedan de una utilización abusiva o ilegítima de la informática. A partir de 1976 se inicia el auge del tratamiento supranacional de la protección de

[198] Herrán Ortiz, A.(1998). Op. cit., p. 56.

la intimidad frente a la informática. Efectivamente, a partir de 1977, la OCDE[199] auspicia un "Encuentro sobre las corrientes internacionales de datos y la protección a la intimidad de las libertades individuales"[200].

Durante 1967, debido a la preocupación por la evolución de las nuevas tecnologías de la información y sus efectos sobre la intimidad de las personas, se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar las tecnologías de la información y su potencial agresividad a los derechos de la persona, cuyo trabajo dio como resultado la Resolución 509 (en el año 1968) de la Asamblea del Consejo de Europa, sobre "los derechos humanos y los nuevos logros científicos y técnicos". Nacía el convencimiento de la necesidad de una exigente regulación uniforme en todos los estados miembros de la Comunidad en defensa de la intimidad de las personas.

Luego, en 1970, el 23 de enero, la Resolución 428 de la Asamblea Consultiva del Concejo de Europa se refiere al Derecho a la Intimidad, como un objeto de obligada protección, frente a la intromisión de la tecnología informática.

En esta línea y asesorados por la Comisión Jurídica de la Asamblea Consultiva, en septiembre de 1973, los parlamentarios recomiendan al Comité de Ministros del Consejo de Europa, que tengan en consideración la iniciativa de adoptar normas protectoras del derecho a la intimidad frente a los avances tecnológicos[201]. Esta norma recomendó a los Gobiernos de sus Estados miembros, respecto de la creación de bancos de datos en el sector privado, considerar determinados aspectos tendientes a tomar precauciones contra todo abuso o mal empleo de la información. Un año más tarde, en septiembre de 1974, se realiza una recomendación similar respecto a la creación de bancos de datos en el sector público[202].

---

[199] Organización para la Cooperación y el Desarrollo Económico: http://www.oecd.org
[200] Herrán Ortiz, A.(1998). Op. cit., p. 58.
[201] Ídem.
[202] El Comité de ministros del Consejo de Europa hizo estas recomendaciones en las resoluciones (73) 22 de 26 de septiembre adoptada durante la 224 reunión de los Delegados de los Ministros,

2.1.- Acuerdo de Schengen de 14 de junio de 1985

El Acuerdo de Schengen[203], firmado en Luxemburgo, constituye uno de los pasos más importantes en la historia de la construcción de la Unión Europea (UE) y también, aunque en forma indirecta, en la evolución del derecho a la protección de los datos de carácter personal[204]. El acuerdo, firmado un 14 de junio de 1985 y en vigor desde 1995, tiene como objetivo finalizar con los controles fronterizos dentro del espacio de Schengen y armonizar los controles fronterizos externos. Al Acuerdo de Schengen se han adherido la mayoría de los Estados miembros de la Unión y algunos terceros países.

En el Título IV del Acuerdo Schengen encontramos disposiciones que organizan la coordinación del control entre los Estados firmantes; entre ellas, el Sistema de Información Schengen (SIS), sistema de información común que permite a las autoridades competentes de los Estados miembros disponer de información relativa a algunas categorías de personas y objetos. Esta información es compartida entre los estados participantes, que son mayoritariamente signatarios del Acuerdo de Schengen (AS), como Alemania, Francia, Bélgica, Países Bajos y Luxemburgo. Después de su creación, varios países se han unido al sistema; Grecia, Austria, Islandia, Suecia, Suiza, Finlandia, Dinamarca, Italia, Portugal, España y Noruega, que firmaron el AS.

El sistema de información Schengen (SIS) permite a las autoridades asignadas por las partes contratantes, gracias a un sistema informatizado, disponer de descripciones de personas y de objetos, con ocasión de controles en las fronteras, aduanas y controles de policía. La base de datos SIS está en Estrasburgo y a ella

---

relativa a la "protección de la vida privada de las personas físicas con respecto a los bancos de datos electrónicos en el sector privado" y (74) 29 de 20 de septiembre, adoptada durante la 236 reunión de los Delegados de los Ministros, con respecto a "la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público". En la primera de las reuniones citadas se adoptó también una Resolución la (73) 23 sobre "medidas de armonización en el ámbito de la Informática Jurídica en los Estados Miembros del Consejo de Europa"

[203] http://www.mir.es/DGRIS/Documentos/Documentos_ambito_europeo/SCHENGEN.pdf http://www.mir.es/SGACAVT/extranje/extschengen/normativa.html (consultado el 24/07/2011).

[204] Rebollo Delgado, L.; Serrano Pérez, M. (2008).Op. cit., p. 41.

tienen acceso todos los estados parte. Cada parte contratante dispone de una oficina SIRENE (*Supplementary Information Request at The National Entry*) cuya finalidad es la preparación de expedientes para la introducción de datos en el SIS y el intercambio de información adicional y para servir de órgano de comunicación bilateral con las SIRENE de otros países.

El SIS sirve además para la búsqueda de personas, objetos, vehículos, armas, billetes y documentos. El sistema ofrece la posibilidad de intercambiar, por vía informática, la información importante. El SIS está compuesto por el sistema de información central (C.SIS), situado en Estrasburgo, y los Sistemas de información nacionales (N.SIS) de las partes contratantes concertados con el C.SIS, que permite a los servicios de policía nacionales competentes consultar la información introducida en el C.SIS.

En el texto del art. 38º se regula la transmisión de datos que puedan ser de interés entre las partes en la lucha contra la criminalidad[205].

[205] Artículo 38 del Acuerdo de Schengen del 14 de junio de 1985:
1. Cada Parte contratante comunicará a toda Parte contratante que lo solicite las informaciones que posea acerca de un solicitante de asilo y que sean necesarias para: - determinar la Parte contratante responsable del examen de la solicitud de asilo; - el examen de la solicitud de asilo; - el cumplimiento de las obligaciones derivadas del presente capítulo. 2. Dichos datos sólo podrán referirse a: a) La identidad (nombre y apellidos, en su caso apellido anterior, apodos o seudónimos, lugar y fecha de nacimiento, nacionalidad actual y anterior del solicitante de asilo y, en su caso, de los miembros de su familia). b) Los documentos de identidad y de viaje (referencia, período de validez, fechas de expedición, autoridad que los haya expedido, lugar de expedición, etc.). c) Los demás elementos necesarios para identificar al solicitante. d) Los lugares de estancia y los itinerarios de viaje.e) Los permisos de residencia o los visados expedidos por una Parte contratante. f) El lugar en que se haya presentado la solicitud de asilo. g) En su caso, la fecha de presentación de una solicitud de asilo anterior, la fecha de presentación de la solicitud actual, el estado actual del procedimiento y el contenido de la decisión adoptada.3. Además, una Parte contratante podrá solicitar a otra Parte contratante que le comunique los motivos invocados por el solicitante de asilo en apoyo de su solicitud y, en su caso, los motivos de la decisión tomada respecto a él. La Parte contratante requerida evaluará si puede acceder a la petición que se le presente. En todo caso, la comunicación de estos datos estará supeditada al consentimiento del solicitante de asilo. 4. El intercambio de información se hará a petición de una Parte contratante y únicamente tendrá lugar entre las autoridades cuya designación haya sido comunicada al Comité Ejecutivo por cada Partecontratante. 5. Los datos intercambiados únicamente podrán utilizarse para los fines previstos en el apartado 1. Dichos datos sólo podrán comunicarse a las autoridades y jurisdicciones encargadas de: - determinar la Parte contratante responsable del examen de la solicitud de asilo; - el examen de la solicitud de asilo; - la puesta en práctica de las obligaciones derivadas del presente capítulo. 6. La Parte contratante que transmita los datos velará por su exactitud y su actualidad. En

En concreto, estamos ante un acuerdo de coordinación y cooperación interestatal, que sin estar dedicado en forma específica a los datos de carácter personal, los afecta directamente y desarrolla el artículo 12 del Convenio 108 del Consejo de Europa de 1981, dedicado al flujo transfrontera de datos de carácter personal. En esta línea, el Título VI del Acuerdo Schengen se ocupa de la protección de los datos de carácter personal; su objetivo es proteger los derechos fundamentales de las personas que figuran en las bases de datos del SIS.

El Acuerdo de Schengen está siendo modificado para incorporar nuevas disposiciones y nuevos miembros; la última modificación fue el 5 de Abril de 2010[206].

En el siguiente título avanzaremos en la evolución del derecho a la protección de los datos de carácter personal y veremos que en 1995, en la Directiva 95/46/CE, también estará presente el tema del flujo de datos transfrontera, en el artículo 25º,

---

el supuesto de que dicho Estado miembro facilitara datos inexactos o que no hubieran debido transmitirse, se informará inmediatamente de ello a las Partes contratantes destinatarias, las cuales estarán obligadas a rectificar dichas informaciones o a eliminarlas. 7. Un solicitante de asilo tendrá derecho a que se le comuniquen, a petición suya, las informaciones que se hayan intercambiado que le conciernan, siempre que las mismas estén disponibles. Si se comprobara que dichas informaciones son inexactas o no hubieran debido transmitirse, tendrá derecho a exigir la rectificación o eliminación de las mismas. Las correcciones se efectuarán en las condiciones establecidas en el apartado 6. 8. En cada Parte contratante de que se trate se dejará constancia de la transmisión y la recepción de las informaciones intercambiadas.9. Los datos transmitidos se conservarán durante un período no superior al necesario para los fines para los que se hubieren intercambiado. La Parte contratante de que se trate estudiará a su debido tiempo la necesidad de conservarlos. 10. En cualquier caso, las informaciones transmitidas tendrán, al menos, la misma protección que la que el Derecho de la Parte contratante destinataria atribuye a las informaciones de naturaleza similar. 11. Si los datos no fueran tratados de forma automática sino de otra forma, cada Parte contratante deberá tomar medidas adecuadas para garantizar el cumplimiento de lo dispuesto en el presente artículo a través de medios de control efectivos. Si una Parte contratante dispusiera de un servicio del tipo mencionado en el apartado 12, podrá encomendar a dicho servicio las funciones de control. 12. Cuando una o varias Partes contratantes deseen informatizar el tratamiento de la totalidad o de parte de los datos mencionados en los apartados 2 y 3, la informatización únicamente estará autorizada si las Partes contratantes interesadas hubieran adoptado una legislación aplicable a dicho tratamiento que cumpla los principios del Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y si hubieran confiado a alguna autoridad nacional adecuada el control independiente del tratamiento y de la explotación de los datos transmitidos de conformidad con el presente Convenio.

[206]Acuerdo de Schengen. Fci.: http://publicaronline.net/2010/04/05/acuerdo-schengen-nuevas-disposiciones-de-visado-para-la-union-europea/ (consultado el 24/07/2011).

con un contenido similar al texto de Schengen, referido en esta norma a la cesión internacional de datos a terceros países no integrantes de la Unión Europea.

2.2.- Directiva 95/46/CE

El 24 de Octubre de 1995, luego de los antecedentes antes mencionados, se aprueba la Directiva europea 95/46/CE, relativa a la protección de las personas físicas en lo referido al tratamiento de los datos personales y a su libre circulación.

La Directiva es una disposición normativa de Derecho comunitario que vincula a los Estados de la Unión o, en su caso, al Estado destinatario en la consecución de resultados u objetivos concretos en un plazo determinado, dejando, sin embargo, a las autoridades internas competentes la debida elección de la forma y los medios adecuados a tal fin[207].

La Directiva 95/46/CE[208]constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador, destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente, encargado de la protección de los mencionados datos.

Establece la Directiva, en su art. 32º, la necesidad de cumplir en un plazo de tres años la acomodación o transposición[209] de su contenido a las normativas nacionales de los Estados miembros[210].

---

[207] http://es.wikipedia.org/wiki/Directiva_(Derecho_de_la_Uni%C3%B3n_Europea) (consultado el 24/7/2011).

[208] http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm (consultado el 24/7/2011).

[209] Transposición: es el mecanismo de derecho comunitario europeo de despliegue y aplicación por las autoridades nacionales competentes (nacional, regional o local) de una norma, la directiva, que además de comunitaria es, por virtud de los Tratados, interna y propia de los ordenamientos

La Directiva 95/46/CE se aplica a los datos tratados por medios automatizados (base de datos informática de clientes, por ejemplo), así como a los datos contenidos en un archivo no automatizado o que vayan a figurar en él (archivos en papel tradicionales). En cambio, no se aplica al tratamiento de datos: a) efectuado por una persona física en el ejercicio de actividades exclusivamente particulares o domésticas; b) aplicado al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, tales como la seguridad pública, la defensa o la seguridad del Estado.

Tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento. Dichos principios se refieren a:

a) La calidad de los datos: los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados.

b) La legitimación del tratamiento: el tratamiento de datos personales sólo podrá efectuarse si el interesado ha dado su consentimiento de forma inequívoca o si el tratamiento es necesario para los siguientes casos: 1. La

---

jurídicos nacionales, pero que requiere de un complemento normativo de los Estados para su efectiva implementación. Se denomina jurídicamente "transposición" al Derecho interno o nacional. Su incumplimiento en cualquier modo (sea por una transposición incorrecta o por su no transposición en absoluto o en el plazo previsto) hace al Estado infractor incurrir en responsabilidad ante las autoridades comunitarias ejecutiva (la Comisión) y judicial (el Tribunal de Justicia), que podrán imponer medidas coercitivas, cuando enuncie derechos de los particulares frente a las administraciones públicas. Esta doctrina permite a los particulares invocar el efecto directo de los preceptos de la directiva que les confieran derechos de forma clara, precisa e incondicional, frente a las administraciones públicas. El Tribunal, no obstante, viene aceptando hasta el momento únicamente el llamado "efecto directo vertical" de las directivas -esto es, en las relaciones entre particulares y administraciones- pero no les ha reconocido efecto directo horizontal alguno (que equivaldría a su inoponibilidadlas relaciones entre particulares). Si este modo de aplicación judicial deviniere por cualquier razón -imputable al Estado- imposible, o fuere, por el contenido concreto de la directiva, difícilmente realizable, los tribunales que conozcan del asunto podrán condenar, en Derecho interno, a la autoridad litigante al pago de la correspondiente indemnización por daños y perjuicios al particular. Todo esto sin perjuicio de las multas que los tribunales comunitarios impongan al Estado infractor a requerimiento de la Comisión Europea. Fci.: http://es.wikipedia.org/wiki/Directiva_(Derecho_de_la_Uni%C3%B3n_Europea)

[210] Rebollo Delgado, L.; Serrano Pérez, M. (2008). Op. cit., p.44.

ejecución de un contrato en el que el interesado sea parte, 2. El cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, 3. Para proteger el interés vital del interesado, o el cumplimiento de una misión de interés público, o la satisfacción del interés legítimo perseguido por el responsable del tratamiento.

c) Las categorías especiales de tratamiento: deberá prohibirse el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. Esta disposición va acompañada de reservas que se aplicarán, por ejemplo, en caso de que el tratamiento sea necesario para salvaguardar el interés vital del interesado o para la prevención o el diagnóstico médico.

d) La información a los afectados por dicho tratamiento: el responsable del tratamiento deberá facilitar cierta cantidad de información (identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, etc.) a la persona de quien se recaben los datos que le conciernan.

e) El derecho de acceso del interesado a los datos: todos los interesados deberán tener el derecho de obtener del responsable del tratamiento:

◦ La confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen y la comunicación de los datos objeto de los tratamientos;

◦ La rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos, así como la notificación a los terceros a quienes se hayan comunicado los datos de dichas modificaciones.

f) Las excepciones y limitaciones: se podrá limitar el alcance de los principios relativos a la calidad de los datos, la información del interesado, el derecho de acceso y la publicidad de los tratamientos, con objeto de salvaguardar, entre otras cosas, la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones penales, un interés económico y financiero importante de un Estado miembro o de la UE o la protección del interesado.

g) El derecho del interesado a oponerse al tratamiento: el interesado deberá tener derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento. También deberá tener la posibilidad de oponerse, previa petición y sin gastos, al tratamiento de los datos respecto de los cuales se prevea un tratamiento destinado a la prospección. Por último, deberá ser informado antes de que los datos se comuniquen a terceros a efectos de prospección y tendrá derecho a oponerse a dicha comunicación.

h) La confidencialidad y la seguridad del tratamiento: las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento. Por otra parte, el responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados.

i) La notificación del tratamiento a la autoridad de control: el responsable del tratamiento efectuará una notificación a la autoridad de control nacional con anterioridad a la realización de un tratamiento. La autoridad de control realizará comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación. Deberá procederse a la publicidad de los tratamientos y las autoridades de control llevarán un registro de los tratamientos notificados.

Las legislaciones nacionales deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados. Además, las personas que sufran un perjuicio como consecuencia de un tratamiento ilícito de sus datos personales tendrán derecho a obtener la reparación del perjuicio sufrido.

Se autorizará la transferencia de datos personales de un Estado miembro a un tercer país que garantice un nivel de protección adecuado; por el contrario, no se autorizará la transferencia a terceros países que no dispongan de tal nivel de protección, salvo contadas excepciones que se enumeran en el texto.

La Directiva pretende facilitar la elaboración de códigos de conducta nacionales y comunitarios que contribuyan a una correcta aplicación de las disposiciones nacionales y comunitarias.

Cada Estado miembro designará una o varias autoridades públicas independientes encargadas de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros en aplicación de la directiva.

También cabe destacar que crea un grupo para la protección de las personas en lo que respecta al tratamiento de datos personales, que estará compuesto por representantes de las autoridades de control nacionales, por representantes de las autoridades de control de las instituciones y organismos comunitarios y por un representante de la Comisión.

Queda claro que esta norma viene a ampliar y a concretar el ámbito que sobre la protección de datos ya había delimitado el Convenio 108 de 1981. La disparidad legislativa de los Estados Miembros así como el desfasaje o la generalidad del Convenio hacían necesaria una normativa más concreta y detallada, un estatuto común sobre la protección de datos y a la preservación de los derechos fundamentales en Europa[211].

[211] Rebollo Delgado, L.; Serrano Pérez, M. (2008). Op. cit., p. 45.

2.3.- Directiva 58/2002/CE del Parlamento Europeo y del Consejo

La Directiva 2002/58/CE[212] del 12 de julio de 2002, forma parte del grupo o paquete normativo de telecomunicaciones, conjunto de disposiciones legislativas destinado a regular el sector de las comunicaciones electrónicas y a modificar a la normativa existente en el sector de las telecomunicaciones. El mencionado paquete normativo de telecomunicaciones comprende cuatro directivas relativas al marco general, al acceso y a la interconexión, a la autorización y a las licencias, y al servicio universal.

En diciembre de 2009, este paquete normativo de telecomunicaciones fue modificado por medio de las Directivas conocidas como "Legislar mejor" y "Derechos de los ciudadanos"; también fue alterado con la instauración de un Organismo de Reguladores Europeos de Comunicaciones Electrónicas (ORECE)[213].

La Directiva 2002/58/CE afecta principalmente al tratamiento de datos de carácter personal en el marco de la prestación de servicios de comunicaciones.

En materia de Seguridad del tratamiento, la Directiva establece que el proveedor de comunicaciones electrónicas está obligado a proteger la seguridad de sus servicios:

1. Garantizando que únicamente accedan a los datos de carácter personal las personas autorizadas;

2. Protegiendo los datos de carácter personal frente a su pérdida o alteración accidental;

[212] Directiva 2002/58/CE de 12 de julio de 2002 (Unión Europea). Fci.: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:es:HTML (Op. cit.: consultada el 20/12/2012)

[213] Organismo de Reguladores Europeos de Comunicaciones Electrónicas (ORECE). Fci.: http://sociedaddelainformacion.wordpress.com/2010/01/28/el-orece-nuevo-regulador-de-las-telecomunicaciones-de-la-union-europea-inicia-su-actividad/ (Op. cit.: Consultado el día 26/7/2001).

3. Garantizando la aplicación de una política de seguridad relativa al tratamiento de datos de carácter personal. En caso de violación de la seguridad de los datos de carácter personal, el proveedor de servicios debe advertir a la persona afectada así como a la Autoridad Reguladora Nacional (ARN).

En materia de confidencialidad, la Directiva recuerda, como principio de base, que los Estados miembros deben garantizar, a través de la legislación nacional, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de comunicaciones electrónicas. En particular, deben prohibir que personas distintas de los usuarios escuchen, intercepten o almacenen comunicaciones sin el consentimiento de los usuarios afectados. El abonado o usuario que almacene información debe ser previamente informado sobre las finalidades del tratamiento de sus propios datos, pudiendo retirar su consentimiento al tratamiento de datos relativos al tráfico.

Con respecto a la retención de datos, la Directiva establece que los datos relativos al tráfico y a la localización deben borrarse o volverse anónimos cuando dejen de ser necesarios para la comunicación o la facturación, salvo en caso de que el abonado haya dado su consentimiento para cualquier otro uso. Por lo que respecta a la problemática cuestión de la retención de datos, la Directiva establece que los Estados miembros solamente pueden limitar las disposiciones en materia de protección de datos para que puedan llevarse a cabo investigaciones de actividades delictivas o para garantizar la seguridad nacional, la defensa y la seguridad pública. Una medida de este tipo sólo podrá adoptarse cuando "constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática", o también para garantizar que los datos de comunicación estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, la Directiva establece un régimen de conservación de datos.

En relación con las comunicaciones electrónicas comerciales no solicitadas, también conocidas como *spamming*[214], la Directiva establece que los usuarios han de dar su consentimiento previo antes de recibir este tipo de mensajes. Este sistema abarca asimismo los mensajes de SMS y los demás mensajes electrónicos recibidos en cualquier equipo terminal, fijo o móvil. No obstante, se han establecido excepciones.

La Directiva prevé que los usuarios deben dar su consentimiento para que se almacene información en su equipo terminal o para que se obtenga acceso a dicha información. Para ello, los usuarios deben recibir información clara y precisa sobre la finalidad del almacenamiento o acceso. Estas disposiciones protegen la vida privada de los usuarios contra programas malintencionados, como los virus o programas espías, pero también se aplican a los programas espías, también llamados chivatos en España o *cookies* en EEUU y Argentina[215].

Con respecto a las Guías públicas, establece que los ciudadanos europeos deben dar su consentimiento previo para que su número de teléfono (fijo o móvil), su dirección electrónica y su dirección postal pasen a figurar en tales directorios telefónicos.

En materia de controles, la Directiva determina que los Estados miembros son quienes deben determinar el régimen de sanciones, incluidas las sanciones penales, en caso de violación de las disposiciones que ella establece, y también deben garantizar que las autoridades nacionales competentes dispongan de las facultades y los recursos necesarios para supervisar y controlar el respeto de las

[214] El *spamming* es el abuso de cualquier tipo de sistema de mensajes electrónicos y, por extensión, cualquier forma de abuso en otros medios como *spam* en mensajería instantánea, en foros, en blogs, en buscadores, en mensajes en teléfonos móviles, etc. Generalmente es originado por el ánimo de lucro de los *spammers*. Actualmente, cualquier tipo de *spamming* está mal visto tanto por personas como por empresas y gobiernos, incluso algunos tipos llegan a ser ilegal en algunos países.

[215] Las *cookies* son datos ocultos intercambiados entre un usuario de Internet y un servidor web que quedan archivados en el disco duro del usuario. Su finalidad inicial era conservar datos entre dos conexiones, aunque también constituyen un medio de control de las actividades del internauta que ha sido objeto de muchas críticas.

disposiciones nacionales que se adopten al efectuar la transposición de la Directiva al derecho de cada Estado.

Aun cuando no estaba previsto, los efectos de esta Directiva superaron su alcance territorial dentro de la Unión Europea y su influencia llegó a la Argentina mediante la sentencia del caso "Halabi, Ernesto c/ P.E.N. - ley 25.873 - dto. 1563/04 s/ amparo ley 16.986", del 24 de Febrero de 2009. En este caso, la justicia argentina hizo lugar al amparista Ernesto Halabi y falló a favor en la primera acción de clase concedida con efecto sobre todas las personas (no sólo del actor). Declaró la inconstitucionalidad de la ley 25.873 por violar el derecho a la protección de los datos personales en el sector de las telecomunicaciones[216]. Volveremos sobre este tema en el capítulo que desarrolla la protección de datos en la República Argentina.

2.4.- Directiva 97/66/ CE

La Directiva 97/66/CE[217] de 15 de Diciembre de 1997 define su objeto en el art. 1º, dirigido a armonizar las disposiciones relativas a la protección de datos de los distintos Estados, con el objeto de garantizar un nivel equivalente de protección de las libertades y de los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que hace referencia al tratamiento de los datos personales en el sector de las telecomunicaciones.

Como acostumbra el derecho comunitario, esta directiva también se ocupa de las definiciones en su artículo 2º, cuestión importante al momento de tomar referencia de términos de compleja comprensión en un sector tan ligado a la tecnología como son las telecomunicaciones.

---

[216] Fallo Halabi, Ernesto c/ P.E.N. - ley 25.873 - dto. 1563/04 s/ amparo ley 16.986.
Fci.: http://www.hfernandezdelpech.com.ar/JurisprudenciaArgFalloHalabi.html (fci:el 25/7/2011). También puede consultarse en: http://www.iprofesional.com/notas/78867-Fallo-Halabi-Ernesto-c-PEN---ley-25873---dto-156304-s-amparo-ley-16986.html (fci: el 17/12/2012).

[217] Fci.: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.5-cp--Directiva-97-66-CE-.pdf (Op. cit.: consultado el 25/7/2011).

El propósito de la Directiva radica en establecer las obligaciones y derechos, tanto de abonados como de proveedores, en el ámbito de las telecomunicaciones y de la protección de los datos personales[218]. Así, el proveedor de un servicio público de telecomunicaciones está obligado a preservar la seguridad de sus servicios, y a organizar la confidencialidad de las comunicaciones que son objeto del servicio. Se limitan en forma taxativa los datos que el proveedor puede almacenar al respecto del usuario, y rige en lo especificado la Directiva 95/46/CE. Con respecto a los datos personales recogidos en las guías impresas o electrónicas accesibles al público, o de posible obtención por los servicios de información, obliga a los proveedores de servicio a limitar el contenido de tales guías a los datos estrictamente necesarios para identificar al abonado concreto, a menos que el abonado haya prestado su consentimiento inequívoco para la publicación de otros datos sobre su persona. También otorga al abonado el derecho a exigir al proveedor que lo excluya gratuitamente de la guía de teléfonos.

El 18 de enero de 2001, la Directiva 97/66/CE fue objeto de debate judicial en la Sentencia del Tribunal de Justicia de las Comunidades Europeas (Sala Cuarta), en el caso Comisión de las Comunidades Europeas contra República Francesa. - Incumplimiento de Estado - Directiva 97/66/CE - Tratamiento de datos personales y protección de la intimidad en el sector de las telecomunicaciones - No adaptación del Derecho interno. - Asunto C-151/00[219].

El TJCE resolvió en este fallo:1) Declarar que la República Francesa ha incumplido las obligaciones que le incumben en virtud del artículo 15 de la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, al no haber puesto en vigor ni comunicado a la Comisión, dentro del plazo fijado, las medidas de adaptación del Derecho nacional a las disposiciones de los artículos 4; apartado 2, 6; apartados 1, 3

[218] Rebollo Delgado, L.; Serrano Pérez, M. (2008). Op. cit., p. 51.
[219] Fci.: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000J0151:ES:HTML (consultado el 25/7/2011).

y 4, 7, 8; apartados 2, 3, 4 y 6, 11; apartado 2, y 12 de la citada Directiva.2) Condenar en costas a la República Francesa.

La cita de este fallo busca mostrar que esta normativa sobre protección de datos no es tan solo declarativa, dado que los tribunales europeos la aplican y la hacen cumplir incluso a poderosos Estados como la República de Francia.

2.5.- Nuevas normas europeas

Internet ha cumplido veinte años desde su apertura al uso masivo y sus efectos, junto a otros fenómenos del mundo de las comunicaciones han potenciado la revolucionaria y vertiginosa evolución del uso de la tecnología.

El uso masivo de la web, de los buscadores y de las redes sociales son tan sólo algunos signos de una realidad de movimiento y cambio tecnológico a la que el Estado moderno y el derecho no deben desatender para dar adecuación permanente de su legislación. Europa, consciente de esta realidad, fue adecuando su legislación de protección de datos personales. Prueba de esta evolución normativa son las ya comentadas Directivas 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones y la Directiva 2002/58/CE, también del Parlamento Europeo y del Consejo de Europa que derogara la Directiva antes mencionada. Podemos ver que la Unión Europea busca constantemente adaptarse a la evolución tecnológica por medio de la modificación de las normas vigentes o a través de la aprobación de nuevas normas reguladoras que protejan a las personas en su derecho a la autodeterminación informativa.

Algunas de las nuevas normas europeas que fueron adecuando el derecho a la protección de los datos de carácter personal al progreso del sector de las comunicaciones, son las siguientes:

a) Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) Nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.

b) Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

c) Por último, la Directiva 2008/68/CE del Parlamento Europeo y del Consejo Europeo de 24 de septiembre de 2008, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.

2.6.- Proyecto de la Comisión Europea del año 2012

La norma básica vigente de la UE en materia de protección de datos es la ya comentada Directiva 95/46/CE, adoptada en el año 1995 con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de estos datos entre los Estados miembros.

Desde la aprobación de la Directiva hasta nuestros días, se ha producido una rápida evolución tecnológica. La acumulación e intercambio de datos se ha

incrementado enormemente y se procesan a gran escala, tanto en el sector de las empresas privadas como en el de las administraciones públicas.

Pese a que los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos en la actualidad, se han presentado una serie de problemas que la Unión Europea no ha logrado resolver con la normativa actual. Entre ellos, la Comisión Europea destaca en su documento de 25 de enero de 2012, COM (2012) 11 final, "la fragmentación en cómo se aplica en la Unión la protección de datos de carácter personal, la inseguridad jurídica y la percepción generalizada de la opinión pública de que existen riesgos significativos, especialmente por lo que se refiere a la actividad en línea". Y expresa que ha llegado el momento "de establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas".

La Comisión Europea consideró que un Reglamento es el instrumento jurídico más apropiado para definir el marco de la protección de datos personales en la Unión. Entiende que la aplicabilidad directa de un Reglamento reducirá la fragmentación jurídica y ofrecerá una mayor seguridad jurídica merced a la introducción de un conjunto armonizado de normas básicas, la mejora de la protección de los derechos fundamentales de las personas y la contribución al funcionamiento del mercado interior.

El Tratado de la Unión Europea establece que a partir del principio de subsidiariedad (artículo 5, apartado 3, del TUE), la Unión solo debe intervenir en caso de que los objetivos perseguidos no puedan ser alcanzados de manera suficiente por los Estados miembros por sí solos, sino que puedan alcanzarse mejor a escala de la Unión. Las razones expuestas anteriormente indican, según el criterio de la Comisión, la necesidad de adoptar iniciativas a escala de la UE por los siguientes argumentos:

- El derecho a la protección de datos de carácter personal, consagrado en el artículo 8 de la Carta de los Derechos Fundamentales, requiere el mismo nivel de protección de datos en toda la Unión. La ausencia de normas comunes de la UE provocaría el riesgo de que hubiera diferentes niveles de protección en los Estados miembros y restricciones en los flujos transfronterizos de datos personales entre los Estados miembros con distintas normas.
- Los datos personales se transfieren a través de las fronteras nacionales, tanto internas como externas, a ritmos cada vez más rápidos. Además, existen retos prácticos a la ejecución de la legislación de protección de datos y la necesidad de cooperación entre los Estados miembros y sus autoridades, que tiene que organizarse a escala de la UE para garantizar la unidad de aplicación del Derecho de la Unión. Por otra parte, la UE es la que está en mejores condiciones para garantizar de forma efectiva y coherente el mismo nivel de protección de los ciudadanos cuando sus datos personales se transfieren a terceros países.
- Por sí solos, los Estados miembros no pueden mitigar los problemas que se plantean en la situación actual, especialmente los debidos a la fragmentación de las legislaciones nacionales. Por tanto, existe una necesidad específica de establecer un marco armonizado y coherente que permita una adecuada transferencia de datos personales a través de las fronteras interiores de la UE, al tiempo que se garantiza una protección efectiva a todas las personas físicas en la UE.
- Las iniciativas legislativas de la UE propuestas serán más efectivas que acciones similares adoptadas a nivel de los Estados miembros debido a la naturaleza y magnitud de los problemas, que no se circunscriben al ámbito de uno o varios Estados miembros.

La regulación propuesta recientemente por la Comisión Europea está basada en un Reglamento que sustituya a la Directiva 95/46/CE, en el que se fija el marco jurídico general de protección de datos de la UE[220].

[220] Junto al nuevo Reglamento, la Comisión propone una Directiva (que sustituye a la Decisión Marco 2008/977/JAI) que fija las normas sobre la protección de los datos personales tratados con

Siguiendo el documento de 25 de enero de 2012 COM (2012) 9 final[221], se exponen los principales componentes de la reforma del marco jurídico para la protección de datos de la UE:

2.6.1.- Control ciudadano

Para reforzar los derechos de los ciudadanos a la protección de sus datos, la Comisión propone nuevas normas que:

a) Aumenten el control de los ciudadanos sobre sus datos:

- asegurando que, siempre que se requiera su consentimiento, este se otorgue de forma explícita, a saber, mediante una declaración o una actuación clara y afirmativa por parte del interesado, y libre;
- dotando a los usuarios de Internet de un derecho efectivo al olvido en el entorno en línea: el derecho a que se supriman sus datos si retiran su consentimiento y no existen otros motivos legítimos para conservarlos;
- garantizando un acceso fácil a los datos propios y un derecho de portabilidad de los datos: el derecho a obtener del responsable del tratamiento una copia de los datos conservados y la libertad de transferirlos de un proveedor de servicio a otros sin trabas;
- reforzando el derecho a la información de tal forma que los ciudadanos comprendan plenamente cómo se tratan sus datos personales, especialmente cuando esas actividades afecten a niños.

b) Mejoren los medios que permiten a los ciudadanos ejercer sus derechos:

- reforzando la independencia y las competencias de las autoridades nacionales de protección de datos de forma que estén adecuadamente equipadas para dar curso eficazmente a las reclamaciones, estén

---

fines de prevención, detección, investigación o persecución de delitos y para las actividades judiciales correspondientes.

[221] *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI*. Bruselas, 25.1.2012 COM (2012) 9 final.

facultadas para llevar a cabo investigaciones efectivas, adopten decisiones vinculantes e impongan sanciones efectivas y disuasorias;

- ensanchando las vías de recurso administrativo y judicial en caso de violación de los derechos de protección de datos. Concretamente, las asociaciones debidamente habilitadas podrán ejercitar acciones judiciales en nombre de los particulares.

c) Refuercen la seguridad de los datos:

- fomentando el uso de tecnologías que protejan la privacidad (tecnologías que, al minimizar la conservación de datos personales, resguardan la privacidad de la información), configuraciones por defecto respetuosas de la privacidad y regímenes de certificación de la privacidad;
- imponiendo a los responsables del tratamiento de los datos una obligación general de notificar, sin demora indebida, toda violación de datos tanto a las autoridades competentes en materia de protección de datos (en un plazo de 24 horas siempre que sea posible) como a los afectados.

d) Acrecienten la responsabilidad de quienes tratan datos, concretamente:

- exigiendo a los responsables del tratamiento de los datos que nombren a un Delegado de Protección de Datos en las empresas con más de 250 empleados y en las empresas que efectúen operaciones de tratamiento de datos que entrañen cierto riesgo;
- introduciendo el principio de «privacidad desde el diseño» a fin de asegurar que las garantías de protección de los datos se incorporan ya en la fase de planificación de los procedimientos y sistemas;
- imponiendo a las organizaciones que lleven a cabo operaciones de tratamiento que entrañen cierto riesgo la obligación de llevar a cabo evaluaciones de impacto sobre la protección de los datos.

2.6.2.- Protección de datos en el mercado digital

Con el fin de potenciar la dimensión de mercado único de la protección de datos, la Comisión propone:

- fijar las normas de protección de datos al nivel de la UE mediante un Reglamento directamente aplicable en todos los Estados miembros, lo que pondrá fin a la aplicación acumulativa y simultánea de distintas leyes nacionales de protección de datos;
- simplificar el entorno regulador mediante una drástica reducción de los trámites burocráticos y la eliminación de determinadas formalidades, como los requisitos generales de notificación; habida cuenta de su importancia para la competitividad de la economía europea, se otorgará especial atención a las necesidades específicas de las microempresas y de las pequeñas y medianas empresas;
- ampliar la independencia y las facultades de las autoridades nacionales de protección de datos, habilitándolas para llevar a cabo investigaciones, adoptar decisiones vinculantes e imponer sanciones efectivas y disuasorias, y obligar a los Estados miembros a que les faciliten los recursos suficientes para el desempeño de esas tareas;
- crear un sistema de *ventanilla única* para la protección de datos en la UE: los responsables del tratamiento de datos de la UE tendrán como único interlocutor a una autoridad nacional de protección de datos, a saber, la del Estado miembro donde esté radicado el establecimiento principal;
- crear las condiciones necesarias para una cooperación presta y eficaz entre autoridades nacionales de protección de datos, lo que incluirá la obligación para cualquiera de ellas de llevar a cabo investigaciones e inspecciones a petición de cualquier otra y el reconocimiento mutuo de sus decisiones;
- crear un mecanismo de coherencia al nivel de la UE para asegurar que las decisiones de las autoridades nacionales de protección de datos que tengan mayor repercusión europea tengan plenamente en cuenta los puntos de vista de las demás autoridades de protección de datos interesadas y se ajusten plenamente al Derecho de la UE;

- elevar el rango del Grupo de trabajo del artículo 29, convirtiéndolo en un Consejo Europeo de Protección de Datos a fin de mejorar su contribución a la aplicación coherente de la legislación en materia de protección de datos y de sentar unas sólidas bases de cooperación entre las autoridades de protección de datos, incluido el Supervisor Europeo de Protección de Datos, y potenciar las sinergias y la eficacia disponiendo que este último asuma las tareas de la Secretaría del Consejo Europeo de Protección de Datos.

2.6.3.- Globalización y protección de los datos

La globalización presenta desafíos que requieren de herramientas y mecanismos flexibles, especialmente para las empresas activas en todo el mundo. Pero también se hacen necesarias nuevas normas que garanticen al mismo tiempo la protección jurídica de los datos personales acorde a los nuevos tiempos. La Comisión propone las siguientes acciones:

- adopción de normas claras que determinen en qué supuestos se aplica el Derecho de la UE a los responsables del tratamiento de datos establecidos en terceros países y que, en particular, especifiquen que siempre que se ofrezcan bienes y servicios a ciudadanos de la UE, o cuando se proceda a algún control de su comportamiento, serán de aplicación las normas europeas;
- toda decisión de adecuación que la Comisión adopte se basará en criterios explícitos y claros;
- la circulación legítima de datos a terceros países se facilitará reforzando y simplificando las normas sobre transferencias internacionales de datos a los países no cubiertos por ninguna decisión de adecuación, y sobre todo racionalizando ciertas herramientas (como por ejemplo las normas corporativas vinculantes) y generalizando su uso, de forma que puedan aplicarse a los responsables del tratamiento de datos y dentro de los grupos de sociedades, lo que reflejará mejor el número de empresas que

llevan a cabo actividades de tratamiento de datos, especialmente mediante computación en nube;

- apertura de un diálogo y, cuando así proceda, negociaciones con terceros países (especialmente los socios estratégicos de la UE y los países de la Política Europea de Vecindad) y con las organizaciones internacionales pertinentes (como el Consejo de Europa, la Organización para la Cooperación y el Desarrollo Económico, las Naciones Unidas) a fin de promover la adopción de unas normas de protección de datos exigentes e interoperables en todo el mundo.

Observamos que la Comisión Europea busca reformar la legislación de la UE en materia de protección de datos para alcanzar una regulación más actual, más consolidada, más coherente y más global, que dé un mayor protagonismo al ciudadano. Se quiere beneficiar con ella en primer lugar a los particulares, ya que consolidará sus derechos a la protección de datos y aumentará su confianza en el entorno digital.

Pero la Comisión Europea también busca con esta reforma beneficiar a las empresas simplificando el marco jurídico existente en materia de protección de datos personales y con ello generar un estímulo para el desarrollo de la economía digital dentro de la UE, siempre con la intención de aumentar la riqueza y los puestos de trabajo en el espacio común.

2.7.- La protección de datos en la Constitución Europea

La Unión Europea también trató la protección de los datos personales en su Constitución aprobada por unanimidad por el Tratado de Roma[222], el 29 de octubre de 2004, por los jefes de Estado o de Gobierno de los Estados miembros de la Unión Europea. El Tratado de Roma establece una Constitución para Europa, por

[222] El Tratado de Roma es el instrumento jurídico que establece la Constitución Europea. El día 29 de octubre de 2004 se procedió a la firma del mismo en Roma, donde se encuentra depositado.

eso es más conocido como Constitución Europea o Tratado Constitucional, cuyo proyecto había sido aprobado el 18 de junio de 2003.

El 12 de enero de 2005, el Parlamento Europeo aprobó una resolución por 500 votos a favor, 137 en contra y 40 abstenciones, en la que recomendó a los Estados miembros que ratificaran la Constitución.

En algunos países, el tratado fue sometido a un referéndum que tuvo resultados distintos y mientras en España los electores lo aprobaron con una baja participación (44%), en Francia y Holanda con una alta participación (69 y 63%, respectivamente) fue rechazado, lo que provocó una crisis institucional europea.

Entró en vigencia el primero de noviembre de 2006.

El Tratado confirma los avances logrados para garantizar la protección del derecho fundamental a la protección de datos personales. Lo sitúa en el artículo II-68, dentro del Título II, que se refiere a las libertades, que a su vez se contienen en la Parte II, que lleva por título "Carta de los derechos fundamentales de la Unión". De este modo, por vez primera, la máxima norma que será de aplicación en todo el territorio de la Unión Europea reconoce expresamente el derecho fundamental a la protección de los datos personales.

El Artículo II-68 Protección de datos de carácter personal de la Constitución de Europa[223], expresa lo siguiente:

> *1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
>
> *2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.*

[223] Constitución Europea. Fci.: http://www.unizar.es/centros/fderez/doc/ConstitucionEuropea.pdf

3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

Como podemos ver, en el derecho comunitario europeo el derecho a la protección de datos personales ha sido ampliamente debatido y legislado. Su importancia radica en la influencia que el derecho comunitario europeo ejerce directamente sobre los estados miembros por el plazo de dos años para transponer las Directivas. Si el Estado miembro de la Unión Europea no transpone una directiva a su derecho interno, esta pasa a formar parte del derecho común de cada Estado al cumplirse el plazo de trasposición de dos años y como tal debe ser aplicada por el juez del lugar.

Por este motivo, se hará a continuación una descripción tan sólo referencial de la legislación y de la jurisprudencia de cada uno de los estados miembros, ya que la importancia de la legislación de la Unión Europea, por las cuestiones antes mencionadas, radica en su poder de armonizar la legislación de los Estados miembros.

En materia de protección de datos personales, la Directiva 95/46/CE fue la encargada de esgrimir este poder armonizador de la legislación sobre los Estados miembros con el fin de eliminar los posibles obstáculos para el flujo de los datos personales; para garantizar un nivel elevado de protección en la Unión Europea, la legislación de protección de datos fue armonizada. Por este motivo, aun cuando muchos de los Estados de la Unión Europea contaban con legislación sobre protección de datos personales antes de la aprobación de la Directiva 95/46/CE, debieron adaptar su legislación interna en la materia, al transponer la directiva. Veamos a continuación los resultados de ese proceso en algunos de los Estados Miembros de la Unión Europea. Decimos algunos y no todos, dado que por dificultades idiomáticas o de acceso a la información, hay algunos de los Estados europeos sobre los que no se encontró información suficiente sobre el tema:

3.- España

El derecho a la protección de los datos personales surgió en España con la Constitución de 1978, ya que los constituyentes españoles de 1978 pensaron que el desarrollo de las nuevas tecnologías de la información y las telecomunicaciones era una amenaza para los derechos fundamentales de los ciudadanos. Para evitar el peligro que les representaba el desarrollo tecnológico de las TIC, incorporaron en la Constitución española, en el artículo 18.4, una garantía de protección a las personas frente a la informática. Esta norma, presente en la Constitución, tiene por objeto limitar el uso de la informática para garantizar el honor, la intimidad familiar y personal de los ciudadanos junto al pleno ejercicio de sus derechos.

Los constituyentes españoles tuvieron a la vista el artículo 35 de la Constitución Portuguesa de 1976 junto a las diferentes leyes ya existentes en algunos Estados europeos, de protección de datos y defensa de la intimidad frente a la informática, por ejemplo las danesas y alemanas, que incidieron en la actitud de los parlamentarios españoles desde los primeros debates sobre la nueva Constitución.

Cinco años más tarde, con el fin de garantizar los derechos y las libertades de las personas físicas, y en particular su intimidad frente a la utilización de la informática, se dio desarrollo legislativo al mencionado artículo 18.4 de la Constitución, por medio de la Ley Orgánica 5/1992 sobre regulación del tratamiento automatizado de datos de carácter personal, promulgada en 1992.

Como consecuencia de los mandatos de la Directiva 95/46/CE, la LORTAD fue derogada y reemplazada en 1999 por la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) Nº 15/1999 vigente en la actualidad, que tuvo como principal objeto adecuar la legislación española a la mencionada Directiva.

Antes de ocuparnos de la LOPD, es necesario un comentario sobre la ley derogada, dado que sus efectos se sintieron tanto dentro como fuera de España y su articulado sirvió de fuente para leyes de otros estados, en particular de

Latinoamérica. A modo de ejemplo podemos mencionar la vigente ley argentina Nº 25.326 de Protección de Datos Personales promulgada en el año 2000, en la cual se observa una fuerte influencia de la LORTAD.

La LORTAD fue la primera ley orgánica española referida a la protección de los datos de carácter personal que vino a cumplir con el expreso mandato constitucional del artículo 18.4, que ordenaba al legislador español que dictara una norma de tutela de las libertades en relación con el uso de la informática, y con diversos acuerdos internacionales que contaron con la adhesión española.

El principal antecedente de la LORTAD es el Convenio de Protección de Datos Personales Nº 108, firmado en el año 1981 por el Consejo de Europa y ratificado por España en 1984. Este Convenio internacional exigía, en el artículo 4º, que los países signatarios incorporaran a su derecho interno las normas necesarias para garantizar la eficacia de los principios consagrados en su texto. A su vez, el 5 de octubre de 1992, la Unión Europea emitió una Directiva referida a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. En igual sentido, el acuerdo de Schengen, suscrito inicialmente por Alemania, Francia y los países de Benelux en 1985, y desarrollado por un convenio de aplicación del 19 de junio de 1990 al que se han adherido otros Estados de la Unión Europea (Italia, Grecia, Portugal, España, etc.), acuerda la supresión gradual de controles entre las fronteras comunes de los países signatarios. Para ello, este acuerdo regula el flujo de informaciones personales en función de la cooperación policial. El Sistema de Información de Schengen (SIS) tiene como objetivo principal la comunicación de informaciones para el control de las personas "indeseables" y/o "inadmisibles" dentro del espacio Schengen con una gran base de datos policiales situada en Estrasburgo y sometida a la legislación francesa de protección de datos personales. Para evitar los efectos nocivos del intercambio de información policial, el convenio de Schengen también exigió que cada país signatario incorporara normas internas sobre protección de datos personales que

satisfagan los principios del Convenio del Consejo de Europa para la protección de datos personales.

Respondiendo a estos compromisos internacionales, la LORTAD buscó garantizar en España los derechos y libertades de las personas físicas y en particular su intimidad frente a la utilización de la informática y además cumplir con el mandato constitucional del artículo 18.4.

En el diseño normativo de la LORTAD, el legislador reunió características de leyes de protección de datos de diferentes generaciones: exige una autorización previa a los bancos de datos (aporte de las leyes de primera generación), da una protección especial a los datos sensibles por su inmediata incidencia en la privacidad o de su riesgo para las prácticas discriminatorias (leyes de segunda generación), y limita la cesión de datos, controlando la dinámica de su uso y funcionalidad (aporte propio de las leyes de tercera generación).

Siguiendo la línea de las leyes de protección de datos de tercera generación, la exposición de motivos de la LORTAD anunciaba la protección de los bancos de datos personales desde una perspectiva funcional que no se limitó a su tutela en cuanto meros depósitos de informaciones, sino como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar un perfil informático personal.

El perfil informático de la persona es considerado, en la exposición de motivos como la reputación o fama, que es expresión del honor y que puede ser valorado favorable o desfavorablemente para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión de determinados colectivos.

La LORTAD buscó también tutelar la calidad de los datos, pero no al dato en sí mismo, sino en función de evitar que su información permita o propicie actividades discriminatorias.

En su estructura normativa se distinguen dos sectores básicos:

a) Una parte general o dogmática, dedicada a la proclamación de la libertad, en la esfera informática, en la pluralidad de sus facultades y manifestaciones, donde se encuentran plasmados los principios de protección de datos con referencia expresa a la calidad de los datos, información y consentimiento del afectado junto a una protección especial de los datos sensibles referidos a la ideología, la religión y las creencias. También otorga una protección media para los datos relativos al origen racial, la salud o la vida sexual;

b) Una parte especial u orgánica en la que se establecen los mecanismos institucionales y la organización que debe supervisar el funcionamiento de las bases de datos a fin de garantizar la libertad informática.

La LORTAD también prohibió el flujo de datos a otros países que no tengan idénticas normas de protección a las existentes en la Unión Europea y ordenó la creación de un organismo regulador independiente, denominado "Agencia de Protección de Datos" con la función de velar por el cumplimiento de las leyes de protección de datos y aplicar sanciones a quienes no cumplan o violen las leyes de protección de datos en España.

En el año 1999, luego de siete años de vigencia de la LORTAD, el parlamento español la derogó y sancionó la Ley 15/99 conocida como LOPD, la cual entró en vigencia luego de su publicación en el Boletín Oficial del Estado, el día 14 de diciembre del año 1999. A partir de la entrada en vigencia de la LOPD, España adecuó su legislación a la Directiva europea 95/46/CE.

Esta nueva ley determina en el artículo 1º que su objeto es garantizar y proteger en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal. A su vez, el inciso a) del artículo 3º determina que "dato de carácter personal es cualquier información concerniente a personas físicas identificadas o identificables".

Puede observarse que mientras en la LORTAD se protegía a las personas sólo del procesamiento automatizado de datos, en la LOPD esta categoría ha dejado de existir y se protege a las personas del tratamiento de todo tipo de datos personales, incluso de aquellos que se encuentran almacenados en archivos o ficheros manuales. La eliminación de la palabra "automatizados" en el objeto de la LOPD cobra importancia al momento de comparar ambas leyes, ya que la desaparición de la distinción entre datos personales automatizados y no automatizados permite que la LOPD alcance a todos los datos de carácter personal en una misma categoría de datos y extienda su objeto a un campo mucho más amplio.

Otra diferencia entre ambas leyes es que mientras la LORTAD buscó cumplir el mandato constitucional de desarrollar el artículo 18.4 de la Constitución para limitar el uso pernicioso de las nuevas tecnologías de la información y las comunicaciones, la LOPD desarrolla toda la sección primera de la Constitución referida a los derechos fundamentales y a las libertades públicas.

Puede observarse que aun cuando la ley 15/1999 establece un objeto con un contenido legal más amplio y ambicioso, aunque menos concreto que el objeto de la LORTAD, no se modifica el concepto de datos personales existente en ambas leyes.

Entendemos como un acierto, que la nueva ley 15/1999 no incluya dentro de su protección a los datos de las personas jurídicas, en coincidencia con los lineamientos de la Directiva 95/46/CE, la cual en su artículo 2º apartado a) define a los datos de carácter personal como toda información sobre una persona física identificada o identificable ("el interesado"). Identificable es toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular por medio de un número de identificación o a través de uno o varios elementos específicos, tales como características de su identidad física, fisiológica, psíquica, económica, cultural o social.

La legitimación activa para accionar recae en la ley 15/1999 en el titular del dato. El artículo 3º de esta ley, dedicado a las definiciones, define en el apartado e)

al afectado o interesado, como toda persona física titular de los datos que sean objeto del tratamiento de datos.

En igual sentido, el apartado c) del artículo 3º define el tratamiento de datos, diciendo que son operaciones y procedimientos técnicos de carácter automatizado que permiten recoger, grabar, conservar, bloquear, cancelar y ceder datos por medio de comunicaciones, consultas, interconexiones y transferencias.

Ya estudiamos en el capítulo I de este trabajo, cómo el Tribunal Constitucional español declaró la inconstitucionalidad de algunos artículos de la ley LOPD, al resolver en el año 2000 un recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. En esta sentencia, el Tribunal Constitucional establece el derecho a la protección de datos como un derecho fundamental autónomo que configura su contenido con los principios y derechos que se contemplan en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, y en virtud del cual, el ciudadano puede decidir sobre sus propios datos y debe ser informado para qué finalidad se obtienen y así consentir sobre la entrega de los mismos para finalidades explícitas. El afectado tiene el derecho de acceder a los datos que tanto empresas, particulares, como Administraciones tengan almacenados sobre su persona, y así, poder rectificarlos o cancelarlos.

La primera parte del apartado 1º del artículo 21 de la Ley Orgánica 15/99 expresa que: "Los datos de carácter personal recogidos o elaborados por las administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas". El Tribunal Constitucional declaró nulo y contrario a la Constitución la parte final del apartado 1º del artículo 21 que continúa expresando "salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso".

Igualmente declara contrarios a la Constitución y nulos los apartados 1º y 2º del artículo 24 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal referido a "Otras excepciones a los derechos de los afectados".

El apartado 1º expresa que "Lo dispuesto en los apartados 1y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas".

El apartado 2º del artículo 24, por su parte expresa: "Lo dispuesto en el artículo 15 y en el apartado 1º del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resulte que los derechos que dichos preceptos conceden al afectado hubieren de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las comunidades autónomas".

Esta sentencia tiene importantes consecuencias, ya que restringe la posibilidad de cesión de datos entre las Administraciones Publicas solo al ejercicio de determinadas competencias y al tratamiento posterior con fines históricos, estadísticos o científicos. Es por ello que, fuera de las excepciones contempladas con carácter general en los artículos 11.2 LOPD y con carácter específico en el artículo 21.1 y 2 LOPD, será siempre necesario el consentimiento de las personas afectadas por los datos, para que las Administraciones Públicas los puedan ceder entre ellas, salvo que expresamente una norma con rango de ley, lo establezca como excepción.

La declaración de inconstitucionalidad de los incisos del apartado 1º del artículo 24 establece que el derecho de información al ciudadano, reconocido en el

artículo 5.1 y 2 LOPD, únicamente podrá ser excepcionado por las Administraciones Públicas, cuando dicha información pueda afectar a la Defensa Nacional, a la seguridad pública, o a la persecución de una infracción de tipo penal.

También suprime todo el apartado 2º del artículo 24, por lo que las únicas excepciones específicas que las Administraciones Públicas podrán alegar para negar el ejercicio de los derechos de acceso, rectificación y cancelación realizados por los ciudadanos, serán las reguladas en el artículo 23 LOPD.

La LOPD ha mantenido una filosofía, impuesta por la LORTAD, según la cual siempre debe haber un responsable frente al daño producido por una posible infracción. En este sentido, la Ley alcanza al responsable del tratamiento de datos, aun cuando no resida en territorio español. Por eso, en caso de que el responsable del tratamiento no esté establecido en territorio de la Unión Europea, la Ley lo obliga a designar un representante en España.

Tanto en la LORTAD como en la LOPD, el artículo 10, distingue claramente la figura del titular del fichero y la figura del responsable del mismo; sin embargo, el resto del articulado, de ambas leyes, no vuelve a repetir esta distinción. Por eso se observa que la LOPD no solo ha desaprovechado la oportunidad para distinguir entre la figura del titular del fichero y el responsable del mismo, sino que en el apartado d) de su artículo 3º aumenta la confusión al aumentar un nuevo nombre y emplear los términos responsable de fichero y responsable del tratamiento para una misma función en la que mezcla características del titular del fichero y del responsable del tratamiento o del fichero.

La LOPD incorpora la nueva figura del encargado de tratamiento, que podría haber servido para superar la confusión del artículo 10º pero no lo hace. Esta nueva figura solo se emplea en el caso de que el tratamiento se realice por cuenta del responsable del tratamiento mediante un contrato, que la LORTAD llamaba prestación de servicios, y es conocido como *out sourcing*. La LOPD otorga a esta

forma de prestación de servicios por terceros, mayor atención que la LORTAD y le dedica el artículo 12, con el título de "Acceso de datos por cuenta de terceros".

La LORTAD limitaba a cinco años el tiempo durante el cual el prestador del servicio podía almacenar los datos mediante autorización del responsable del fichero. La LOPD no establece tiempo alguno, por lo que se presume que podrán almacenarse en tanto sean necesarios para la prestación periódica del servicio.

El tercero prestador de servicios, también conocido como outsoucer, no asumía, en la LORTAD, ninguna responsabilidad frente a la Agencia de Protección de Datos, por el contrario, solo se limitaba a responder por las responsabilidades derivadas del contrato suscripto con el responsable del fichero.

En este tema la LOPD ha prestado más atención a la figura del prestador de servicios, y cambia el criterio de la LORTAD, ya que considera responsable del tratamiento al encargado del tratamiento, con las responsabilidades correspondientes a dicha condición en los siguientes casos: a) cuando destine los datos a finalidad distinta de la estipulada en el contrato; b) cuando comunique los datos; c) cuando utilice los datos incumpliendo las estipulaciones del contrato.

En la antigua ley 5/1992 era fácil conocer si un tipo de registro era una fuente accesible al público, ya que definía a las fuentes accesibles al público como aquellos ficheros automatizados de titularidad pública cuyo objeto legalmente establecido fuese el almacenamiento de datos para su publicidad con carácter general. Esto cambia en la LOPD, ya que para evitar las dudas que la LORTAD generaba en el pasado, establece un numerus clausus de fuentes accesibles al público.

La LOPD evolucionó positivamente al considerar fuentes accesibles al público, solo a las siguientes bases de datos: a) Censo promocional; b) Repertorios telefónicos (normativa específica); c) Listas de personas pertenecientes a grupos profesionales (limitado a: nombre, título, profesión, actividad, grado académico,

dirección e indicación de su pertenencia al grupo); d) Diarios oficiales; e) Boletines oficiales; f) Medios de comunicación.

Con esta enumeración taxativa de las fuentes accesibles al público se han despejado las dudas que se planteaban en la LORTAD sobre la existencia de un archivo determinado que contenía o no datos accesibles al público.

Mientras la LORTAD prohibía el uso de los datos personales para finalidades distintas a las declaradas, la LOPD prohíbe las finalidades incompatibles, sin mencionar a las finalidades distintas.

Con respecto a la seguridad de los datos, el artículo 9 de la LOPD ha incluido entre los responsables de adoptar medidas de seguridad necesarias al responsable de tratamiento o responsable de fichero y al encargado de tratamiento, figura a la cual la ley le da la misión de efectuar el tratamiento por encargo del responsable del fichero mediante un contrato.

La LOPD ha sido criticada por referirse, en algunos artículos, a un concepto con un nombre, y luego, en otro artículo, al mismo concepto con otro nombre distinto. De esta forma se facilita la confusión al momento de aplicar la ley. A modo de ejemplo, podemos citar el cambio del término "cesión de datos" por "comunicación de datos", ya que este cambio de nombre no se mantiene en todos los artículos.

La LOPD otorga a las personas los derechos a la impugnación de valoraciones, consulta, acceso, rectificación y cancelación, oposición, tutela e indemnización. En este punto la LOPD ha incorporado, como novedad, el derecho de oposición que se configura como el derecho que tienen los interesados, en determinadas circunstancias, a oponerse al tratamiento de los datos que les conciernen, en cuyo caso, previa petición y de forma gratuita serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, con su simple solicitud.

Emilio Del Peso Navarro entiende que para poder ejercer el derecho de oposición, el afectado ha de reunir dos requisitos: a) Que existan motivos fundados y legítimos; b) Que éstos estén referidos a una concreta situación personal. Cumplidas estas circunstancias, el responsable del archivo o fichero deberá excluir del tratamiento los datos relativos al afectado.

Con respecto al derecho a la impugnación de valoraciones que en la LORTAD se circunscribe a las producidas por un tratamiento automatizado, en la LOPD es más general y abarca cualquier tipo de tratamiento, siendo aún más amplia que la Directiva Europea, que también alcanza solo a los datos automatizados.

El apartado 1º del artículo 13, sólo se refiere al tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. Entendemos que esto es un tanto ambiguo y enormemente subjetivo, lo que puede llegar a producir inseguridad jurídica.

En la LOPD, el derecho de acceso se regula como un derecho gratuito, cosa que no hacía la LORTAD, y el responsable del archivo debe responder informando los datos de caracteres personales solicitados, junto al origen de los datos y de las cesiones realizadas o las que se tenga previsto realizar.

La LOPD introduce el derecho de rectificación y cancelación con un plazo de 10 días para hacerlos efectivos. La doctrina española ha criticado esta técnica legislativa, por considerar que no deben introducirse plazos en la ley, sino que deben ser fijados por la normativa de reglamentación. Sin embargo, hay coincidencia en la insuficiencia del plazo de 5 días que establecía el artículo 15.2 del Real Decreto 1332/94, que desarrollaba determinados aspectos de la LORTAD; pero Emilio del Peso Navarro expresa en su crítica que se podría haber introducido la modificación del plazo en una Disposición Transitoria hasta tanto se modifique el plazo en el reglamento citado.

Con respecto a los códigos tipos, la LOPD amplía la posibilidad de aplicar los mismos a los ficheros de titularidad pública y asimismo a las organizaciones en

que se agrupen los responsables del tratamiento tanto de estos archivos como de los archivos de titularidad privada.

La LOPD hace hincapié en el derecho de los interesados a que sus datos no figuren en las listas profesionales y en el censo promocional y en aquél se prevé la circunstancia de que pueda figurar en las listas que una persona determinada no desea recibir publicidad.

En los artículos correspondientes al movimiento internacional de datos se enumeran las circunstancias que debe evaluar la Agencia de Protección de Datos para que el nivel de protección que ofrece un país se considere adecuado. Al respecto se amplían las excepciones a la ley en este tema, siguiendo la Directiva Comunitaria con una detallada casuística.

La Ley Orgánica de Protección de Datos de Carácter Personal 15/99 recibió críticas de la doctrina española por la prisa con que fue debatida y sancionada. El olvido de rectificaciones, el cambio de nombre de un concepto para luego usar nuevamente el anterior y en definitiva desaprovechar una nueva ocasión para dictar una legislación cuidada que proteja integralmente a los ciudadanos en su intimidad, son algunas de las consecuencias que la doctrina atribuye al apuro de un debate parlamentario poco profundo y a la prisa en su sanción. Sin embargo, y aun a pesar de la exigente crítica de los doctrinarios españoles, no sería justo dejar de reconocer que tanto la LORTAD como la LOPD, son leyes que modelaron la legislación del mundo de habla hispana, y en especial la legislación Sudamérica, en la materia.

4.- Alemania

Alemania cuenta con el antecedente de haber legislado la primera ley europea de las llamadas leyes de primera generación de protección de datos en el Estado de

Hesse. Promulgada el 7 de octubre de 1970[224], esta norma provincial fue precursora en su tiempo y solitaria en su territorio[225].

En esta ley del *Land de Hesse*, se encuentra la primera referencia a un Comisario de Protección de Datos que sólo podrá ser cesado en su cargo, en caso de probarse ciertos supuestos de hecho que justificarán la separación del servicio, garantizando de esta forma su independencia, ya que la ley expresaba textualmente: "no estará sujeto a órdenes o instrucciones de órgano alguno". En la actualidad existen leyes similares en múltiples Länder de la antigua RFA, normas que siguiendo el antecedente de la antigua ley de Hesse, hacen gala de independencia y federalismo.

El Estado Federal Alemán tuvo que esperar casi siete años hasta que se promulgó, el 27 de enero de 1977, la Ley Federal para la protección contra el uso ilícito de Datos Personales[226].

En la actualidad, la ley de protección de datos en Alemania es la conocida BDSG de 20 de diciembre de 1990[227] que entrando en vigor el 1 de junio de 1991 sustituye a la de enero de 1977 y su objeto es "Proteger al individuo para que la utilización de los datos personales no comporte un atentado a su derecho a la personalidad".

La BDSG[228], parte como principio general de que el tratamiento de datos personales está prohibido salvo en los casos en que se autorice expresamente o cuando el afectado ha dado su consentimiento. Aun cuando el principio del consentimiento es base de esta ley, su rigidez es atenuada por reglas muy flexibles

[224] En esa fecha Alemania todavía no estaba unificada.
[225] Davara Rodríguez, M. Op. Cit. (1998); p. 63.
[226] Quiroga Lavié, H. *Habeas Data*. Editorial Zavalía,Buenos Aires, 2001, p. 19.
[227] Promulgada el 20 diciembre de 1990 (BGBl. I S. 2954, Boletín Oficial Federal I, p. 2954), refundida por la notificación de fecha 4 de enero de 2003 (BGBl. I S. 66, Enero de 2003, Boletín Oficial Federal I, p. 66).Modificada por el artículo 5 de la Ley de 29/07/2009 (Boletín Oficial Federal I, p. 2254), (BGBl. I, S. 2355 [2384], Boletín Oficial Federal I, p. 2355 [2384] y por la ley vom 14.08.2009 (BGBl. I, S. 2814) de fecha 08/14/2009 (Boletín Oficial Federal I, p. 2814).
[228] Ley de Protección de Datos Personales alemana (BDSG):
Fci: http://www.gesetze-im-internet.de/bdsg_1990/

que permiten el tratamiento de datos de carácter personal sin consentimiento de su titular en múltiples casos.

Fuera de las excepciones mencionadas, sólo se podrá sortear el consentimiento del titular por medio de una ley del Estado o cuando un interés superior esté en juego y en todo caso se establece dentro de las disposiciones generales el secreto profesional que garantice, aun con el tratamiento de los datos, unos niveles mínimos de confidencialidad.

Las oficinas públicas pueden recolectar y reproducir información, solo en cumplimiento de sus misiones específicas. La creación de un registro público debe ser comunicada al ciudadano y publicada en el Boletín Oficial, con excepción de las cuestiones relacionadas con el servicio de información federal, con el servicio de seguridad militar, con la defensa de la Constitución Federal y la defensa nacional.

De igual forma, por regla, la seguridad debe establecerse en el tratamiento de datos, como garantía para el ciudadano.

El sistema de protección de los datos personales de la ley alemana no es de aplicación a las personas jurídicas, quedando una referencia expresa a su aplicación solamente a las personas físicas al definir los datos objeto de protección como los concernientes a las informaciones individuales sobre la situación personal o material de una persona física determinada o determinable.

La ley se aplica a todo tipo de registro, sean automáticos o manuales, públicos o privados, siempre que en ellos se procesen datos personales[229]. El objeto de la ley se extiende también a los archivos manuales cuando los datos se encuentren bajo una estructura lógica que permita que sean objeto de tratamiento automatizado. La ley textualmente dice: Toda colección de datos estructurados de la misma forma y susceptibles de ser clasificados, tratados y explotados según unos criterios definidos. Los archivos o registros de datos necesitan autorización legal para su habilitación.

[229] Quiroga Lavié, H. (2001). Op. cit., p. 28.

La ley federal se aplica al sector público tanto a la administración federal como a la de los *Länder*, siempre que en estos no existan leyes particulares propias, y al sector privado, teniendo, al igual que las leyes de Argentina y de España, un capítulo dedicado a los archivos de titularidad pública y otro capítulo independiente dedicado a los de titularidad privada.

El Registro de Bancos de Datos Automáticos está a cargo de un funcionario calificado como Delegado Federal para la Protección de Datos Personales, el cual es designado por el Presidente de la República. El sistema distingue los Bancos de Datos denominados propios, que no poseen regulación de ningún tipo, con mínima intervención de la autoridad.

Una orientación de utilidad o permisividad para el desarrollo de la función administrativa se muestra, en lo relativo a los ficheros de titularidad pública, al afirmar que está permitido recoger datos personales cuando su conocimiento sea necesario para la realización de las obligaciones legales del organismo que recoge los datos.

La calidad de los datos se rige bajo unas normas de exactitud y transparencia en su tratamiento, en el conocimiento de la finalidad del mismo, y con un tiempo limitado de conservación o mantenimiento de los datos en el archivo. Se establecen normas tanto para los ficheros de titularidad pública como para los de titularidad privada.

Toda persona que estime lesionado un derecho como consecuencia del tratamiento de los datos que le conciernen puede recurrir al Comisionado Federal para la Protección de Datos y Libertad de Información[230] o a la autoridad de tutela local.

Cuatro son las posibilidades, con diferentes funciones (a veces repetidas) que se encuentran reguladas en la normativa alemana sobre la autoridad de control.

[230] Comisionado Federal para la Protección de Datos y Libertad de Información.
Fci.: www.datenschutz.bund.de (último ingreso el 22/7/2011).

En primer lugar el Delegado Federal para la protección de datos que, elegido por el parlamento alemán (*Bundestag*) a propuesta del Gobierno por mayoría absoluta y para un período de cinco años con garantías de independencia, vela por el respeto a la ley de las administraciones federales, interviene de oficio a instancia de parte y tiene acceso a todos los documentos que tengan relación con el tratamiento automatizado de datos de carácter personal. También y en forma similar al Director de la Agencia Española de Protección de Datos, el Delegado alemán, tiene que realizar una memoria anual que debe remitir al Parlamento todos los años.

En segundo lugar, encontramos los Comisarios encargados de la protección de datos de cada uno de los *Länder*. Cada *Land* tiene su legislación específica en materia de protección de datos personales y el Comisario de Datos funciona como una autoridad de tutela local que realiza la misma función referida o con relación y competencia a los archivos de titularidad pública del *Land*. En tercer lugar, están los funcionarios encargados de la seguridad de los datos que actúan en el sector privado de forma que las empresas con un número mínimo de empleados que realicen un tratamiento automatizado de datos de carácter personal, están obligadas a nombrar una persona que vela por el cumplimiento de la ley en el ámbito de la empresa con unos fines claros de seguridad en el tratamiento y de cumplimiento de la normativa.

Por último, encontramos a las autoridades de tutela sobre los datos privados de cada *Land*. Ante estas autoridades de tutela se puede presentar cualquier persona que considere que sus derechos están siendo conculcados por una entidad privada. Puede acudir a esta autoridad de tutela que posee las mismas facultades de control con el delegado federal, pero sólo interviene a instancia de parte.

En el ámbito de las sanciones, éstas pueden ser de carácter económico para cubrir también el monto de las indemnizaciones por daños y los intereses correspondientes o bien pueden ser de carácter penal con penas de prisión. El responsable del tratamiento de los datos tiene la carga de la prueba.

Como ya adelantamos, la supervisión de las actividades de los registros de datos privados la realiza un ombudsman, comisario o controlador de la protección de datos, nombrado por cada empresa encargada de su procesamiento por medios automáticos, siempre que en el banco de datos intervengan más de cinco empleados. Existen penas de arresto y multa para los casos de incumplimiento de la ley.

La parte tercera de la BDSG está consagrada al tratamiento de datos personales realizado por entidades no públicas y empresas regidas por el derecho público que participan en concursos públicos.

En concreto, el art. 28 está dedicado a la recogida, comunicación y uso de datos para fines propios y especifica que la recogida modificación o comunicación de datos personales o su uso como medio para realizar uno de los fines de una empresa propia será permisible en los casos que este artículo enumera, entre los que son de destacar los siguientes:

a) Cuando los datos se recojan y traten como consecuencia de los fines propios de una relación contractual o cuasi-contractual entre el responsable del tratamiento y el afectado.

b) Cuando sea necesario para salvaguardar los intereses legítimos del responsable del fichero y no exista razón para pensar que los intereses legítimos del afectado en impedir dicho tratamiento o uso serían superiores al del responsable, con lo que se busca encontrar un equilibrio de intereses que permita el tratamiento sin que pueda ser bloqueado por un interés individual.

c) Cuando los datos puedan ser obtenidos de fuentes accesibles al público o si el responsable del tratamiento tuviera derecho a publicar dichos datos, a no ser que el interés legítimo del afectado en impedir un tratamiento o uno de esos datos sea manifiestamente superior al del responsable.

En todo caso los datos han de ser recogidos de buena fe.

El art. 29 de la BDSG regula el tratamiento de datos personales con el fin de comunicación de dichos datos, la llamada "cesión de datos". Una permisividad para el tratamiento de los datos, y su posterior cesión con ánimo de lucro se encuentra en este artículo, siempre que se cumplan determinadas características que podemos resumir de la siguiente forma:

a) No hay razón para presumir que el afectado tiene un interés legítimo en impedir el tratamiento o alteración de sus datos o

b) Los datos personales pueden obtenerse de fuentes generalmente accesibles al público o

c) El responsable del tratamiento tiene derecho a publicar los datos, a no ser que el interés legítimo de afectado manifiestamente excluya la posibilidad de tratar o alterar sus datos.

El segundo apartado del art. 29 centra su atención sobre la comunicación de los datos a terceros, inclusive como negocio, con un legítimo fin de lucro, que será permisible si se cumplen las dos condiciones siguientes:

- el destinatario de los datos ha demostrado un interés legítimo plausible en conocer esos datos y

- no hay razón para suponer que el afectado tiene un interés legítimo en impedir la comunicación de dichos datos.

La forma de conjugar estas características de equilibrio entre los diferentes intereses en juego, debe buscarse en la referencia del artículo 28 al tratamiento y uso de datos personales con el fin de comunicación a un tercero.

Esto puede resumirse así:

- Art. 28 (3) si el afectado se opone al uso o comunicación de sus datos con los fines citados, el uso o comunicación para dichos fines no estará permitido.

- Art. 28 (4) el destinatario de los datos puede tratarlos o usarlos para el fin para el que le han sido comunicados. El tratamiento o uso de esos datos con otro fin sólo estará permitido si se cumple alguna de las condiciones del art. 28 (1)

Las instituciones u organismos que se dedican al tratamiento de datos personales como negocio con el fin de comunicarlos a terceros deberán notificar a la autoridad de control competente (el comisario del Land correspondiente) el comienzo y la finalización de las operaciones de tratamiento de datos en el período de un mes.

El capítulo II de la BDSG está dedicado a los derechos del afectado. En él se protegen los siguientes derechos:

a) Información cuando los datos se recogen y tratan por primera vez. Existen varias excepciones o modificaciones que afectan a la comunicación de tal forma que no es necesaria en todos los casos, o que pueda ser eludida en determinadas circunstancias, como por ejemplo, por las autoridades responsables de las tareas relativas a la seguridad nacional o a la lucha contra el crimen, o por las autoridades financieras para lo relativo a sus funciones de control. De igual manera, en el sector privado se debe atender al hecho de que la comunicación o el contenido de la información no atente gravemente o comprometa en el mismo sentido los objetivos comerciales del poseedor de la información.

b) Acceso, bajo petición del afectado, a las informaciones que le conciernan; en ese caso la comunicación será gratuita.

c) Rectificación de datos inexactos, destrucción de datos que no deben figurar y bloqueo de los datos. El bloqueo se producirá cuando existan dudas sobre la exactitud de los datos o cuando haya que completar garantías para su tratamiento.

Finalmente, cabe destacar el aporte realizado a la evolución del derecho a la protección de datos personales por Alemania desde la jurisprudencia de su Tribunal Constitucional, ya que desde sus célebres sentencias marcó el rumbo en la evolución de este derecho. En particular cabe destacar la sentencia del Tribunal Constitucional alemán sobre la ley del censo en 1983.

En este fallo el TC alemán sentó las bases de la doctrina de la autodeterminación informativa.

5.- Austria

La República de Austria, miembro de la Unión Europea desde 1995, ratificó el Convenio del Consejo de Europa[231] el 30 de marzo de 1988, el cual entró en vigor el 1 de julio del mismo año.

Austria ya había dictado su Ley de Protección de Datos Personales, conocida en alemán con el nombre de *Datenschutzgesetz* (DSG, 1978), el 18 de octubre de 1978. Más tarde, esta ley fue adaptada a través de modificaciones como la realizada por la decisión 609/1989 de la Corte Constitucional[232] y últimamente a través de la Ley Federal de Protección de Datos de Carácter Personal (*Bundesgesetzüber den Schutz personen bezogener Daten / Datenschutzgesetz 2000*[233] *- DSG 2000)* dictada en el año 2000[234], se adaptó la legislación austríaca en materia de protección de datos a la Directiva 95/46/CE de Parlamento y del Consejo de Europa.

[231] El texto del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (hecho en Estrasburgo el 28 de Enero de 1981), fue publicado por la Agencia de Protección de Datos (España) "El Consejo de Europa y la Protección de Datos Personales". Editado por la Agencia de Protección de Datos; impreso por De Arellano, Madrid, 1997, página 13 y sucesivas.
[232] Davara Rodríguez, M. *La protección de datos en Europa*. Editorial Asnef-Equifax. Publicación de la Universidad Pontificia Comillas. Madrid; 1998, p. 70.
[233] Ley Federal de Protección de Datos Personales del año 200.
[234] Se puede encontrar información actualizada sobre la legislación de protección de datos personales de Austria en la página web www.kronegger.at

Con respecto al derecho fundamental a la protección de los datos personales, el artículo 1º de la ley austríaca del año 2000, textualmente expresa: *"(Disposición Constitucional). Derecho Fundamental a la Protección de Datos:*

1. (1) Todas las personas tienen el derecho al secreto de los datos personales que le conciernen, sobre todo en lo que respecta a su vida privada y familiar, en la medida en que exista un interés que merezca protección. Tal interés queda excluido cuando los datos no pueden estar sujetos al derecho al secreto debido a su disponibilidad general o porque no se puede regresar nuevamente a la protección de datos (afectado).

(2) Los datos personales se deben utilizar a favor del interés vital del interesado o con su consentimiento, las restricciones al derecho al secreto sólo se permiten para salvaguardar los legítimos intereses primordiales de otro, es decir, en caso de una intervención de una autoridad pública, la restricción sólo se permitirá sobre la base de las leyes necesarias por las razones indicadas en el art. 8, párr. 2 del Convenio Europeo de Derechos Humanos (Gaceta de Leyes Federales N º 210/1958). Dichas leyes podrán establecer el uso de los datos que merecen una protección especial sólo para salvaguardar importantes intereses públicos y establecerán las garantías adecuadas para la protección de los intereses de los interesados en el secreto. Incluso en el caso de las restricciones permitidas en la intervención con el derecho fundamental se llevará a cabo utilizando sólo la menos invasiva de todos los métodos efectivos."[235].

Como podemos observar en la transcripción del artículo 1º de la Ley de Protección de Datos de la República de Austria, sus disposiciones permiten recoger y tratar datos personales solamente cuando sea necesario para los fines legales de la organización que lleva a cabo dicha operación. En la práctica, autoriza a llevar a cabo cualquier actividad de recogida y tratamiento de datos, más aún porque la ley no prevé rígidas sanciones en el caso de su cumplimiento.

[235] Véase el sitio web de la Comisión de Protección de Datos de Austria.
Fci.: https://www.dsk.gv.at/ (consultado el 30 de Julio de 2011).

El principio permisivo de la acumulación y el tratamiento de datos personales, se encuentra recogido en el artículo 17 de la Ley de Protección de Datos (*Datenschutzgesetz)* y se refiere exclusivamente a archivos de titularidad privada. Para poder recoger este tipo de datos personales en un archivo de titularidad pública será necesario crear una ley especial, como lo exige el artículo 6 de la norma de Protección de Datos

El artículo 17 de la *Datenschutzgesetz* indica, concretamente, que pueden tratarse datos personales cuando el contenido y el fin del tratamiento sea necesario para los fines legales de la persona, llevando a cabo este tratamiento y los intereses de las personas afectadas, especialmente el derecho a la protección de su intimidad, de forma que no sean violados.

En otras palabras, hay que tener en cuenta dos elementos: a) El fin del tratamiento, que ha de ser legal, y b) los intereses de las personas cuyos datos personales son tratados.

Puesto que las organizaciones que se dedican profesionalmente a recoger estos datos los suelen vender, se interpreta generalmente que su actividad económica es el "fin legal" del tratamiento.

Esta ley se aplica tanto al sector público como al privado; protege tanto a las personas físicas como a las personas jurídicas y actúa sobre cualquier tipo de archivos, siempre que se encuentren automatizados, con excepción de los archivos privados que se utilicen solamente con fines personales.

Los archivos deben ser inscriptos en una oficina de estadísticas[236] creada con el objeto de su control y publicidad. Toda persona interesada puede consultar los archivos de esta oficina y conocer los datos de estructura e identificación de los que se hallen inscriptos, así como la identificación del titular del fichero.

[236] Davara Rodríguez, M. Op. cit., p. 71.

El derecho del ciudadano a exigir la confidencial del tratamiento y comunicación de los datos que le conciernan y, muy especialmente, a los referentes a su vida privada y a su familia, es elevado a la calidad de constitucional, como derecho fundamental. Este derecho no tiene otra limitación que los intereses legítimos de terceros o cuando así se contemple en una ley.

En el caso de los archivos de titularidad pública, la ley exige para su autorización, la necesidad absoluta del tratamiento automatizado de los datos para poder cumplir con las funciones que tiene encomendada la administración de que se trate, a no ser que exista una ley que indique otra cosa.

El artículo primero contempla el derecho de información y comprende la identificación de la persona que realiza el tratamiento, el contenido de los registros, así como el fin que se persigue y la utilización que se realiza de los datos. El derecho de rectificación es elevado a la calidad de constitucional (corregir los datos inexactos y suprimir los que son indebidamente utilizados).

El derecho de acceso es gratuito y debe ser atendido por el responsable del fichero en el plazo máximo de cuatro semanas, siendo su responsabilidad probar la exactitud de los datos que contiene.

No se pueden ejercer los derechos de acceso y de rectificación cuando se trate de datos que afecten a la defensa nacional, a órganos constitucionales y a cuestiones sobre delincuencia o referidas al derecho penal.

Las condiciones para recabar los datos, con una mención específica sobre la pertinencia y finalidad, y, en el sector público, una exigencia -a falta de disposición legal que lo autorice- a la necesidad absoluta para cumplir con las funciones que el órgano tiene encomendadas, destacan en la ley.

Esta ley se encuentra orientada a garantizar un tratamiento legal de los datos de carácter personal en los archivos del sector público, con una remisión a la jurisdicción ordinaria cuando se trate de datos de carácter personal que figuren en

ficheros de titularidad privada, a los que hace una referencia sobre principios y derechos, generalista pero ambigua, y una remisión a los tribunales ordinarios para el procedimiento de control.

La Comisión de Protección de Datos de Austria[237] (*Datenschutzkommission*, en alemán) es la autoridad gubernamental encargada de supervisar la protección de datos personales en Austria; es el equivalente de los comisionados nacionales, autoridades reguladoras o de aplicación en materia de protección de datos que existen en otros países. Cabe remarcar que la Comisión de Protección de Datos en Austria actúa también como autoridad de control de la protección de datos personales en el sector público y sobre las autoridades públicas.

Es una institución independiente, desvinculada del poder judicial, y ante ella toda persona que se considere lesionada por un tratamiento automatizado efectuado por un órgano del sector público puede acudir a la Comisión. Esta comisión solamente actúa con respecto a los archivos de titularidad pública, a instancia de parte, siendo sus resoluciones apelables ante los tribunales administrativos o ante la Corte Constitucional.

Está garantizada la independencia de sus miembros, que no reciben orden o instrucción de nadie y que deben realizar un informe anual a la Asamblea o al Gobierno.

No existe ninguna autoridad de control con respecto a archivos de titularidad privada; los litigios relativos a este tipo de archivos han de resolverse, entonces, por la vía judicial. En el ámbito de los archivos de titularidad privada, por tanto, son competentes los tribunales ordinarios que imponen resoluciones sobre daños y perjuicios.

Existe también un órgano consultivo que se conoce con el nombre de Consejo de la protección de datos, compuesto por quince miembros que representan

[237] Véase nota sobre el sitio web de la Comisión de Protección de Datos Personales de Austria. Op. cit., fci.: https://www.dsk.gv.at .

los partidos políticos, los representantes sociales, los *Länder* y las colectividades locales. Esta institución emite, espontáneamente o a petición de parte, informes y recomendaciones destinadas a los órganos públicos.

Las sanciones previstas consisten en multas y en penas privativas de la libertad que pueden alcanzar la pena de prisión de hasta un año.

El tratamiento de datos sobre incumplimiento de obligaciones dinerarias es una actividad bastante extendida en Austria y sucede, en la mayoría de los casos, sin consentimiento de la persona en cuestión.

La organización más importante en Austria dedicada al tratamiento de información sobre crédito es la *Kreditschutzverband von 1870*. Esta organización recoge primordialmente datos sobre empresas, pero también recoge datos personales sobre personas físicas, especialmente en lo relativo a incumplimiento de obligaciones dinerarias.

No es necesario cumplir ningún requisito especial para hacerse socio del *Kreditschutzverband von 1870*; cualquier persona puede hacerse socia de esta organización y tener acceso a la información que ella trata.

Los bancos austríacos poseen asimismo una lista negra de "clientes indeseables". Con este propósito, los bancos intercambian y tratan información sobre clientes que tienen deudas importantes. En la práctica sucede con frecuencia que las personas incluidas en esta lista no son aceptadas como clientes o se les deniegan créditos, sin que el banco les explique el motivo de esta negativa, basada fundamentalmente en la inclusión de su nombre en la citada "lista negra".

Por otro lado, los registros de embargos de los tribunales austríacos se han hecho accesibles al público. Esto significa que cualquier persona puede controlar si este tipo de procedimiento ha tenido lugar con relación a alguien en concreto; entre otras cosas, es posible saber si una persona ha incumplido una obligación dineraria y si dicho incumplimiento ha sido a una sentencia de las autoridades judiciales.

6.- Bélgica

El Reino de Bélgica[238] comenzó promulgando disposiciones específicas sobre protección de datos para ofrecer garantías a las personas que figuraban en determinados ficheros. De esta forma estableció una conciencia sobre protección de datos personales que formó la base para la posterior aceptación del ciudadano, de una legislación sobre principios y derechos a la autodeterminación informativa[239].

En materia de acuerdos internacionales, Bélgica suscribió el ya estudiado Convenio 108 del Consejo de Europa, ratificado el 28 de mayo de 1993, que entró en vigor el 21 de septiembre del mismo año.

La normativa sobre la protección de datos personales en Bélgica[240] es la Ley del 8 de diciembre de 1992, modificada por la ley de Transposición (de fecha 11 de diciembre de 1998) de la Directiva 95/46/CE, que entró en vigor el 1 de Septiembre de 2001.

La ley no distingue entre ficheros de titularidad pública y ficheros de titularidad privada, extendiendo su alcance a todos los archivos de datos de carácter personal relativos a personas físicas. Quedan fuera de su ámbito de aplicación los ficheros referentes a datos de personas jurídicas, los que mantienen las personas físicas para uso familiar, los que contienen datos públicos y los del órgano estatal destinado a la estadística oficial.

Los principios y derechos generalmente establecidos en estas normativas son recogidos en la legislación belga mediante los llamados derechos de acceso, rectificación y supresión. En ellos se establece que "todas las personas tienen derecho al respeto de su vida privada en el tratamiento de los datos personales que

[238] El Reino de Bélgica es un país soberano miembro de la Unión Europea situado en el noroeste europeo. Cubre una superficie de 30.528 kilómetros cuadrados y posee una población aproximada de 11 millones de habitantes.
[239] Davara Rodríguez, M. (1998). Op. cit., p. 75.
[240] Legislación belga de protección de datos personales. Consultar el sitio web de la Comisión para la Protección de la Vida Privada, autoridad de control en el Reino de Bélgica. Fci.: www.privacy.fgov.be (Consultado el 30 de Julio de 2011).

les conciernan", datos que deben cumplir unos requisitos de adecuación al fin, proporcionalidad y exactitud; datos que deben ser recabados de forma leal y lícita, garantizándose la seguridad y confidencialidad del tratamiento; debe exigirse una conservación de los datos en el fichero que quede limitada en el tiempo de acuerdo a los fines para los que fueron recogidos; se establece también el deber de secreto profesional.

La Autoridad de control en Bélgica es la Comisión para la Protección de la Vida Privada[241], la cual juega un papel muy importante con relación a los archivos de incumplimiento de obligaciones dinerarias. Los consumidores pueden dirigirse a la Comisión, una vez que reciben la notificación de su inclusión en uno de estos archivos, para que ésta investigue la legalidad de dicha inclusión y, en su caso, emita una recomendación dirigida al responsable del archivo.

La Comisión no está autorizada a emitir su opinión sobre la oportunidad de la inclusión de los datos del afectado en algunos de estos archivos, sino que sólo puede pronunciarse sobre la legalidad de dicha inclusión.

Los consumidores pueden dirigirse a la Comisión tanto por carta como por teléfono o fax, para hacer preguntas o exponer su situación concreta. La Comisión recibe anualmente un gran número de quejas de consumidores que afirman haber sido incluidos injustamente en un fichero sobre incumplimiento de obligaciones dinerarias.

La Comisión ha elaborado asimismo diversas notas para informar al público de las disposiciones de la ley de crédito al consumidor de 12 de junio de 1992 y de los derechos que la ley de protección de datos de 8 de diciembre de 1992 les concede con respecto a los ficheros sobre incumplimiento de obligaciones dinerarias en los que sus datos personales han sido registrados.

[241] Comisión para la Protección de la Vida Privada (autoridad de control en materia de protección de datos personales del Reino de Bélgica). Fci: www.privacy.fgov.be (último ingreso el 30 de julio de 2011).

La persona afectada puede dirigirse a la Comisión para la Protección de la Vida Privada, que puede emitir la recomendación al responsable del tratamiento. La Comisión crea un registro nacional de personas físicas y está encargada de velar por el respeto de la vida privada en el funcionamiento de los ficheros. Está compuesta por juristas, por miembros de comités de supervisión creados por leyes específicas y por miembros designados por mayoría por el Parlamento.

La Comisión no tiene potestad sancionadora específica y aunque puede intervenir, por propia iniciativa o a petición de parte, para responder a aquellas cuestiones relativas a la aplicación de los principios fundamentales, realizando las comprobaciones que considere necesarias en los ficheros, con una función inspectora que pueda estar apoyada en la ayuda de expertos, e incluso, cumplir con la misión de mediación y denuncia de las infracciones cometidas, sin embargo solamente podrá remitir una recomendación al responsable del tratamiento.

Respecto de los archivos sobre cumplimiento o incumplimiento de obligaciones dinerarias, no se encuentran regulados en la ley de protección de datos, sino en la ley de crédito al consumidor de 12 de junio de 1991[242], parcialmente reformada el 6 de julio de 1992.

De acuerdo con lo especificado en esta ley de crédito al consumidor, las entidades de crédito están obligadas a comunicar a la central de crédito a particulares del Banco Nacional de Bélgica todo incumplimiento de una obligación dineraria que responda a las siguientes características:

1. El incumplimiento se deriva de una compra a plazos, un préstamo o crédito, o cualquier otra forma de crédito cuyo pago se realice en plazos periódicos, siempre y cuando estos plazos sean iguales durante toda la duración del crédito y una de las siguientes tres condiciones se cumpla:

Cuando tres plazos no hayan sido pagados en su fecha de vencimiento o hayan sido pagados de forma incompleta; o cuando un plazo que ha vencido no ha

[242] Diario oficial belga de 9 de julio de 1991, p. 15203 y siguientes. Fci.: http://www.moniteur.be/.

sido pagado en un plazo de tres meses o haya sido pagado de forma incompleta; o cuando los plazos aún no vencidos sean exigibles inmediatamente en aplicación del artículo 29 de la ley de crédito al consumidor de 12 de junio de 1992.

El artículo 29 de esta ley estipula que la entidad de crédito pueda exigir el pago inmediato de los plazos ya vencidos cuando el consumidor no ha pagado dos o más plazos y habiéndole sido notificado dicho incumplimiento por medio de una carta certificada de la entidad de crédito, no ha cumplido con su obligación en el mes siguiente a la recepción de la notificación.

2. El incumplimiento se deriva de cualquier tipo de crédito no mencionado en los apartados 1 y 3, y una de las siguientes dos condiciones se cumple:

Cuando el consumidor, en incumplimiento del acuerdo de crédito, no ha saldado completamente la deuda existente en un período de tres meses a partir de la fecha en la que la entidad de crédito se lo ha requerido por escrito.

Cuando la entidad de crédito, en aplicación del artículo 59.3 de la ley de crédito al consumidor, ha interrumpido la provisión de dinero al consumidor.

El artículo 59.3 de esta ley dispone que, cuando la entidad de crédito dispone de información de la que puede deducir que el consumidor no está en situación de seguir cumpliendo con sus obligaciones dinerarias, está autorizada a interrumpir la provisión de dinero al consumidor, siempre y cuando éste sea informado por medio de carta certificada con al menos siete días de antelación.

3. El incumplimiento se deriva de un crédito hipotecario y una de las dos condiciones siguientes se cumple:

Cuando el consumidor no ha saldado una cantidad debida en los tres meses siguientes a la fecha de su vencimiento.

Cuando el consumidor no ha saldado una cantidad debida en el mes siguiente al envío por correo certificado de la notificación mencionada en el artículo 45 de la ley de 4 de agosto de 1992 relativa al crédito hipotecario.

El artículo 45 de esta ley especifica que en el caso de impago de una cantidad debida a la entidad hipotecaria en los tres meses siguientes a la fecha de vencimiento, esta entidad debe hacer llegar al consumidor por correo certificado un escrito en el que se le informa de las consecuencias que se derivan de su impago.

La mayoría de las entidades de crédito belgas prevén en sus contratos crediticios la posibilidad de comunicar los incumplimientos mencionados en los apartados 1,2 y 3 a instituciones de carácter privado, siendo las más conocidas B.V.K.[243] y COBAC[244].

Las personas cuyos datos personales han sido recogidos en un fichero sobre incumplimiento de obligaciones dinerarias regulado por la ley de crédito al consumidor pueden ejercer los derechos derivados de la ley belga de protección de datos, de 8 de diciembre de 1992, dirigiéndose al responsable del tratamiento en cuestión, al presidente de un juzgado de primera instancia o a la Comisión para la Protección de la Vida Privada.

Las personas afectadas pueden dirigirse a la entidad de crédito que les concedió un crédito o a su entidad aseguradora. Por medio de una petición firmada y fechada, el afectado podrá consultar los datos personales que con respecto a él tiene registrados esta entidad.

Las personas afectadas podrán dirigirse asimismo a los responsables de ficheros sobre incumplimiento de obligaciones dinerarias tales como el Banco Nacional de Bélgica o instituciones privadas como B.V.K.

---

[243] Unión Profesional de Crédito (Bélgica). B.V.K. es su sigla, responde a este nombre en neerlandés, idioma nacional Belga: *Beroepsvereniging van hetKrediet*.
Fci.: http://www.upc-bvk.be/

[244] COBAC (entidad de crédito de Bélgica). Fci.: http://assecuranz.kompass.com/en/Belgium/Euler-Cobac%20Belgium%20SA-NV/BE504431-dir.php .

La persona afectada podrá consultar los datos personales que con respecto a él tienen registradas estas entidades dirigiendo una carta certificada a la entidad en cuestión, acompañada de una fotocopia de su documento nacional de identidad.

El afectado puede exigir a esta entidad que los motivos del incumplimiento sean comunicados igualmente a las terceras personas, tales como otras instituciones de crédito, instituciones que expiden tarjetas de crédito, etc., a las que dicho incumplimiento sea comunicado.

En ambos casos, el afectado tiene derecho a exigir sin coste alguno de su parte, la corrección o la supresión de aquellos datos que sean incorrectos o erróneos. Para ellos, deberá acompañar a su petición una copia del contrato de crédito o de otro documento que permita a la entidad de crédito identificar sin ningún género de duda el crédito al que la persona afectada se refiere.

El afectado deberá ejercer sus derechos en primer lugar frente a su institución de crédito, puesto que:

La institución que le ha concedido el crédito es la única que tiene a su disposición el contrato de crédito cuyo incumplimiento ha sido registrado.

Los responsables de ficheros de incumplimiento de obligaciones dinerarias (el Banco Nacional de Bélgica, B.V.K., COBAC) a los que datos incorrectos o erróneos han sido comunicados, no tienen derecho a exigir a la entidad que concedió el crédito a la persona afectada documentación que justifique el incumplimiento que ésta les comunica.

Si la persona afectada ejerce su derecho de corrección frente a su entidad de crédito, ésta deberá comunicar las correcciones o supresiones que han tenido lugar a los responsables de ficheros de incumplimiento de obligaciones dinerarias, a los que los datos personales en cuestión habían sido comunicados anteriormente, en un plazo de un mes a partir del día en que la corrección o supresión ha tenido lugar.

En el caso de que su petición de acceso, corrección o supresión de datos personales le sea denegada o cuando no obtenga respuesta alguna en el plazo de sesenta días, la persona afectada puede:

Iniciar un procedimiento frente al presidente de un juzgado de primera instancia, siguiendo el procedimiento indicado en el artículo 14 de la ley de protección de datos de 8 de diciembre de 1992.

Dirigirse a la Comisión para la Protección de la Vida Privada, que puede emitir una recomendación al responsable del tratamiento. En este caso la persona afectada deberá comunicar a la Comisión los hechos irregulares que han tenido lugar y presentar toda la documentación (contrato de crédito, pruebas de pago, correspondencia, etc.) que pueda resultar útil para analizar la situación a la que su queja se refiere.

Estos dos procedimientos no afectan al derecho de la persona titular del dato, de iniciar un procedimiento judicial ante los tribunales, que serán la única institución competente para reconocerle su derecho a obtener, en su caso, una indemnización por los daños causados por la entidad de crédito en cuestión.

Efectos de una petición de corrección o supresión o de la iniciación de un procedimiento frente al presidente de un juzgado de primera instancia.

A partir del momento en que recibe una petición de corrección o supresión del afectado, o es informado de la iniciación de un procedimiento frente al presidente de un juzgado de primera instancia, el responsable del archivo de información sobre incumplimiento de obligaciones dinerarias deberá especificar en cada comunicación de datos a un tercero que el dato ha sido cuestionado por el afectado.

Como se deduce de lo anteriormente dicho, los archivos sobre incumplimiento de obligaciones dinerarias son una práctica habitual en Bélgica, que ha sido claramente incentivada por la ley de crédito al consumidor, que pretende

evitar el endeudamiento de los consumidores y proteger a las entidades de crédito frente a la insolvencia de aquellos.

7.- Dinamarca

El Reino de Dinamarca[245] ratificó el Convenio del Consejo de Europa el 23 de octubre de 1989, entrando en vigor el 1 de febrero de 1990 y consecuentemente legisló sobre protección de datos personales, siendo su actual ley Nº 429[246] del 31 de mayo de 2000, que entró en vigor el 1 de julio de ese año y recibió diferentes modificaciones[247].

En el capítulo I, en su artículo 1º, la ley 429 del año 2000 establece el ámbito de aplicación, expresando que abarcará el tratamiento de datos personales, total o parcialmente automatizado, y el tratamiento no automatizado de datos personales que forman parte de un sistema de base de datos.

El capítulo II se ocupa en el apartado 3 de las definiciones, entre las que destaca el concepto de dato personal como aquel dato relativo a una persona natural identificada o identificable.

Los antecedentes legislativos de la actual ley danesa son importantes, ya que hasta el año 2000, la protección de datos personales en Dinamarca estuvo legislada en dos leyes del 8 de Junio de 1978[248]: la ley 294 aplicable a los archivos de

[245] Dinamarca es una monarquía constitucional desde 1849, fecha en la que quedó abolida la monarquía absoluta que había regido el país desde 1660, y se convirtió en monarquía parlamentaria en 1901. Forma parte de la Unión Europea.

[246] El texto completo de la ley Nº 429 del 31 de mayo de 2000, puede ser consultado en castellano en la siguiente dirección web (fci.): http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/(último ingreso el 4 de Agosto de 2011).

[247] La ley Nº 429 del año 2000 de Protección de Datos personales del Reino de Dinamarca fue modificada por el artículo 7 de la Ley Núm. 280 del 25 de abril de 2001, la sección 6 de la Ley Núm. 552 del 24 de junio de 2005, la sección 2 de la Ley Núm. 519 del 6 de junio de 2007, la sección 1 del Ley Nº 188 de 18 de marzo de 2009 y la sección 2 de la Ley Núm. 503 del 12 de junio de 2009.

[248] Las antiguas leyes danesas del 8 de Junio de 1978 contenían principios de finalidad y proporcionalidad, así como de tiempo de conservación limitado y confidencialidad. Estas dos leyes también establecían los derechos de acceso a la información en forma escrita y rápida tras la

titularidad pública[249]y la 293 referida a los archivos de titularidad privada[250]. En el año 2000 entró en vigor la nueva ley danesa de protección de datos, con el objetivo dar cumplimiento a la Directiva 95/46/CE sobre la protección de las personas con respecto al tratamiento de datos personales ya la libre circulación de estos datos.

---

solicitud, los derechos de cancelación y de rectificación, encontrándose un derecho de acceso indirecto por intermedio de un médico para los datos clínicos. Permitía que la información fuese suministrada verbalmente. El derecho de acceso podía ser denegado en razón de un interés público o privado superior.

[249] La Ley N° 294 de 8 de junio de 1978 sobre los registros públicos entró en vigor el 1 de enero de 1979 y fue modificada por la Ley n°383 de 10 de junio de 1987; fue consolidada en la versión n° 654, del 20 de septiembre de 1991. La ley centraba su ámbito de aplicación en "los registros informatizados que fueren llevados por cuenta de la administración pública y que contuvieren datos personales" y regula las cuestiones específicas a: La creación de los registros (capitulo 2); a los datos que se pueden recabar ("solo podrán registrarse aquellos datos que guarden una clara relación con el desempeño de las funciones de la autoridad correspondiente"), y su conservación (capitulo 3); al acceso de los afectados a los datos que se refieren a ellos (capitulo 4); a la comunicación de datos a particulares (capitulo 5); a la comunicación de datos a autoridades públicas (capitulo 6); a otras cuestiones sobre el cumplimiento y control de la normativa así como a las sanciones que hubiera lugar. Respecto de la creación de ficheros de titularidad pública se establecen unas garantías centradas en la aprobación del Ministro competente después de la consulta al Ministro de Economía, o por la autoridad local competente, estableciendo que ningún fichero puede operar sin que la autoridad responsable haya dado instrucciones sobre su estructura y funcionamiento. Estas instrucciones se remiten a la Comisión de control y, en caso de desacuerdo, el Ministro competente decidía.

[250] La Ley N° 293 del 8 de junio de 1978 sobre los registros privados del Reino de Dinamarca entró en vigor el 1 de enero de 1979, luego fue modificada por la Ley N° 383 del 10 de junio de 1987, versión consolidada con el N°622, de 2 de octubre de 1987. Esta ley regulatoria de los bancos de datos del sector privado distinguía el tratamiento de datos de carácter personal, realizando una separación por capítulos, relativa a los datos tratados por empresas mercantiles, por oficinas de información sobre solvencia, por empresas dedicadas al tráfico de direcciones y distribución de impresos, por oficinas de servicios informáticos y tratamiento automatizado de datos en el extranjero. Para todos estos casos se establecía el principio del consentimiento, los requisitos para el tratamiento de los datos, la forma en que pueden ser recabados, los derechos de acceso, rectificación y, en su caso, cancelación, teniendo la particularidad de establecer requisitos para cada uno de los capítulos, con las excepciones al consentimiento y las cuestiones determinantes del ejercicio de los derechos propios de la clase o categoría en la que se encuentre el titular del archivo y de las características del tratamiento o, adecuación a la necesidad del mismo, o el interés que se encontrara en juego, ya sea que se tratara (el titular del archivo)de empresas mercantiles, de oficinas de información sobre solvencia, de empresas dedicadas al tráfico de direcciones y distribución de impresos, o de oficinas de servicios informáticos.

De esta forma se puede estudiar en forma independiente las características del tratamiento de acuerdo con los intereses en juego y con la particularidad del titular del archivo y su incidencia económica, social u otras. Los archivos privados no se sometían en esta ley a ninguna formalidad en su creación, con la excepción de las agencias de información sobre solvencia y las de servicios informáticos que debían ser registradas ante la Comisión de Protección de los Datos Personales.

La autoridad de control danesa es la Agencia de Protección de Datos Personales, llamada *Data Surveillance Authority*[251], su nombre puede traducirse como Autoridad de Vigilancia de los Datos[252], también conocida bajo el nombre genérico de inspección de registros, está compuesta por un presidente y seis miembros, nombrados por cuatro años por el Ministro de Justicia y tiene como funciones velar por el cumplimiento y la correcta interpretación de las dos leyes. En la actual ley danesa del año 2000 se encuentra contemplada en el Capítulo 16, punto 55.

La Agencia danesa de protección de datos actúa de oficio o a petición de parte; tiene encomendada la misión de indicar a las autoridades responsables de los archivos públicos toda irregularidad de la que tenga conocimiento así como proponer las medidas para su corrección.

A solicitud del interesado, la *Data Surveillance Authority* puede ordenar la rectificación o la supresión de los datos de un archivo privado. Además, tiene competencia para recabar cualquier información que fuera de importancia para su función inspectora y, previa identificación y sin mandamiento judicial, podrán entrar en cualquier local desde el cual el registro fuere administrado o pudiere ser utilizado. A su vez, puede remitir a la autoridad responsable del registro y al ministro competente un informe sobre las infracciones probadas cometidas contra la ley, así como sobre las deficiencias observadas. Podrá también formular a la Autoridad que haya dictado las normas de organización y funcionamiento vigente, en los archivos de titularidad pública, propuestas de modificación de dichas normas.

En el caso de los archivos de titularidad privada, podrá requerir que se cancele el registro o cesión de datos que no debieran tener lugar y que sean cancelados los registros existentes que fueran llevados en contra de las disposiciones de la ley.

[251] Data Surveillance Authority (autoridad de control danesa); en castellano Agencia de Protección de Datos Personales de Dinamarca. Fci.: http://www.datatilsynet.dk/eng/.
[252] Davara Rodríguez, M. (1998). Op. cit., p. 84.

Del mismo modo que lo establece la ley española, está obligada a remitir un informe anual de sus actividades y gestión al Parlamento. La Ley sobre tratamiento de datos personales está bajo la autoridad de la Agencia de Protección de Datos, por lo tanto, es deber de la agencia garantizar que la ley sea respetada. Tal función se cumple en parte por proporcionar orientación y asesoramiento a las autoridades, empresas y ciudadanos.

A través de notificaciones y autorizaciones, la Agencia Danesa de Protección de Datos controla algunos de los procesos más sensibles de los datos personales que se llevan a cabo por las autoridades y las empresas. En caso de quejas de los ciudadanos, la Agencia Danesa de Protección de Datos puede tomar decisiones de acuerdo con las normas de la Ley de Protección de Datos de Carácter Personal. La Agencia Danesa de Protección de Datos también puede ocuparse de casos por iniciativa propia, si por ejemplo, debido a una investigación sobre un ciudadano o artículo de periódico, la agencia sospecha de una violación de las regulaciones de la Ley de Protección de Datos de Carácter Personal.

La Agencia Danesa de Protección de Datos lleva a cabo una serie anual de inspecciones de las autoridades públicas y empresas privadas que han recibido la autorización de la agencia para procesar los datos personales. La Agencia Danesa de Protección de Datos inspecciona si el tratamiento de los datos se lleva a cabo de conformidad con la Ley de Procesamiento de Datos de Carácter Personal.

Si la Agencia Danesa de Protección de Datos descubre violaciones punibles de la Ley de Protección de datos personales en relación con el trámite de una queja o una inspección, está autorizada a emitir un aviso de prohibición o de ejecución o denunciar la violación a la policía.

Las personas domiciliadas en el extranjero también pueden obtener ayuda de la Agencia de Protección de Datos Personales Danesa, pero las solicitudes deben ser planteadas en danés o en inglés.

8.- Francia

En la República de Francia, la protección de los datos de carácter personal se encuentra reglada por la ley n° 78-17[253] del 6 de enero de 1978 relativa a la informática, a los ficheros y a las libertades. Esta ley se aplicaba tanto a los archivos de titularidad pública como a los de titularidad privada, estableciendo para los de titularidad pública que sean creados mediante una ley o un acto reglamentario realizado tras informe motivado de la Comisión Nacional de la Informática y las Libertades[254].

La norma mencionada sufrió modificaciones en el año 2004por imperativo de la Directiva europea 95/46/CE, del Parlamento y del Consejo Europeo, que ordenó a todos los Estados Miembros, incluso a Francia, modificar su legislación en materia de Protección de Datos personales. Al traspasar la mencionada directiva europea fue necesario modificar la antigua ley 78/17 y entró en vigencia la actual ley el 6 de agosto del año 2004.

El Convenio 108 del Consejo de Europa fue ratificado el 24 de marzo de 1983, entrando en vigor el 1 de octubre de 1985. Para adaptarse a la Directiva europea 95/46/CE, la ley de protección de datos personales de Francia del año 1978 fue modificada por la ley relativa a la protección de las personas físicas respecto a los tratamientos de datos de carácter personal del 6 de agosto de 2004. La ley vigente, con las modificaciones de año 2004, cuenta con 72 artículos de los cuales vamos a comentar sólo los principales[255].

---

[253] La ley N° 78-17 del 6 de enero de 1978, relativa a la informática, a los ficheros y a las libertades (Francia), se compone de 48 artículos, que se encuentran distribuidos en siete capítulos, los cuales se titulan: Capítulo I (Principios y Definiciones); Capítulo II (De la Comisión de Informática y Libertades; Capítulo III (Formalidades previas a la puesta en marcha del tratamiento automatizado de datos); Capítulo IV (Recolección, registro y conservación de las informaciones nominativas); Capítulo V (Ejercicio del derecho de acceso); Capítulo VI (Disposiciones Penales); Capítulo VII (Disposiciones varias).

[254] Davara Rodríguez. M. (1998). Op. cit., p. 136.

[255] El vigente texto de la ley N° 78-17 del 6 de enero de 1978, relativa a la informática, a los ficheros y a las libertades (Francia) con la modificación del año 2004, puede encontrarse con traducción al castellano en el sitio web: http://www.cnil.fr/fileadmin/documents/es/Lei78-17VE.pdf (último ingreso el 14 de agosto de 2011).

La ley dedica su capítulo primero a enumerar unos principios y definiciones entre los que destaca la declaración de que "la informática deberá estar al servicio del ciudadano. Su desarrollo debe llevarse a cabo en el marco de la cooperación internacional. No debe perjudicar ni la identidad humana, ni los derechos humanos, ni la intimidad de las personas, ni las libertades individuales o públicas" (art. 1). Podemos observar que este artículo habla del ciudadano en su primera frase y que luego pareciera ampliar la protección a todas las personas, al considerar que es un derecho humano. Esta posición es ratificada en el art. 2º *in fine* cuando expresa: "La persona afectada por el tratamiento de datos de carácter personal será aquélla a la se refieran los datos objeto de tratamiento".

El antes mencionado art. 2º es un artículo de definiciones, que vamos a mencionar textualmente para comprender los alcances de la ley: "La presente Ley se aplicará tanto a los tratamientos automatizados de datos de carácter personal como a los tratamientos no automatizados de datos de carácter personal contenidos o destinados a figurar en ficheros, con exclusión de los tratamientos realizados en el ejercicio de actividades exclusivamente personales, cuando el responsable de los datos cumpla las condiciones previstas en el artículo 5 (ámbito de aplicación del derecho nacional).Constituirá un dato de carácter personal cualquier información relativa a una persona física identificada o identificable, directa o indirectamente, con referencia a un número de identificación o a uno o varios elementos propios de esta persona. Para determinar si una persona es identificable, se deberá tomar en consideración el conjunto de medios de los que dispone o a los que puede tener acceso el responsable del tratamiento o cualquier otra persona para permitir la identificación. Constituirá un tratamiento de datos de carácter personal cualquier operación o conjunto de operaciones sobre dichos datos, sea cual fuere el procedimiento utilizado, y especialmente la recogida, la grabación, la organización, la conservación, la adaptación o la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso, el cotejo o la interconexión, así como el bloqueo, el borrado o la destrucción. Constituirá un fichero de datos de carácter personal cualquier conjunto

estructurado y estable de datos de carácter personal, accesibles según determinados criterios. La persona afectada por el tratamiento de datos de carácter personal será aquella a la que se refieran los datos objeto de tratamiento".

A partir de la modificación del año 2004, el art. 3º se ocupa de la figura del responsable del fichero, expresando que: "I. – El responsable de un tratamiento de datos de carácter personal será, salvo designación expresa en las disposiciones legales o reglamentarias relativas a dicho tratamiento, la persona, la autoridad pública, el servicio o el organismo que determine sus finalidades y sus medios. II. – El destinatario de un tratamiento de datos de carácter personal será cualquier persona habilitada para recibir comunicación de dichos datos que no sea la persona afectada por el tratamiento, el responsable del tratamiento, el subcontratista y las personas que, por sus funciones, están encargadas del tratamiento de los datos. No obstante, las autoridades que, en el marco de una misión particular o del ejercicio de un derecho de comunicación, estén legalmente habilitadas para solicitar al responsable del tratamiento la comunicación de datos de carácter personal, no tendrán la consideración de destinatarios".

El capítulo segundo de la ley francesa describe las condiciones de licitud de los tratamientos de datos de carácter personal, y en tal sentido exige determinadas condiciones. Textualmente el inciso 1º del art. 6º exige que los datos sean "*recogidos y tratados leal y lícitamente*".

El segundo inciso del artículo antes mencionado ordena que los datos sólo se recojan para finalidades determinadas, explícitas y legítimas y que no sean tratados ulteriormente de manera incompatible con dichas finalidades. No obstante, un tratamiento ulterior de los datos con fines estadísticos o con fines de investigación científica o histórica será considerado compatible con las finalidades iniciales de la recogida de los datos, si se realiza respetando los principios y procedimientos previstos en la ley (capítulos II, IV, V, IX y X).

En los incisos 3º y 4º del art. 6º, la ley manda que los datos recogidos sean adecuados, pertinentes y no excesivos con respecto a las finalidades para las que hayan sido recabados y a sus posteriores tratamientos; que sean exactos, completos y, si es necesario, actualizados; que se tomen medidas apropiadas para que los datos inexactos o incompletos con respecto a las finalidades de recogida o de tratamiento, sean borrados o rectificados. Sobre la conservación de los datos, el inc. 5º ordena que se haga de tal manera que permitan la identificación de los interesados durante un plazo que no exceda del que sea necesario para cumplir las finalidades para las que hayan sido recogidos y tratados.

Mientras la antigua la ley francesa N° 78-17[256] no exigía como regla general el consentimiento del afectado para poder tratar datos personales, ya que en su art. 16 establecía como único requisito previo al tratamiento de datos personales, en archivos de titularidad privada, la declaración ante la autoridad de control francesa (Comisión Nacional de la Informática y de las Libertades)[257], tal declaración implicaba el compromiso del responsable del tratamiento de satisfacer todas las exigencias de la ley. Actualmente este principio ha cambiado, puesto que en la vigente ley modificada en el año 2002, en el art. 7 se expresa textualmente sobre la vigencia del principio del consentimiento atenuado por expresas excepciones. Leamos el artículo 7º:"Cualquier tratamiento de datos de carácter personal requerirá el consentimiento del interesado o deberá ajustarse a una de las siguientes condiciones: 1°. El cumplimiento de una obligación legal a la que esté sujeto el responsable del tratamiento; 2°. La salvaguarda del interés vital del interesado; 3°. El ejercicio de una misión de servicio público que le incumba al responsable o al destinatario del tratamiento; 4°. La ejecución, bien de un contrato del que interesado sea parte, bien de medidas precontractuales adoptadas a petición del mismo; 5°. La satisfacción del interés legítimo perseguido por el responsable del tratamiento o por

[256] Gozaíni, O. *Derecho Procesal Constitucional*. *Habeas Data. Protección de datos Personales. Doctrina y Jurisprudencia*. 1ª ed. Editorial Rubinzal –Culzoni Editores. Buenos Aires, 2001. Junto a esta obra, se acompaña un CD-ROM en el cual se encuentra el texto de la ley 78/17 traducido al castellano. ISBN: 950-727345 (la edición no publicación la catalogación de este libro).
[257] Commission Nationale de L`Informatique et des Libertés. Fci.: http://www.cnil.fr/ (último ingreso el 2 de Septiembre de 2011).

el destinatario, siempre y cuando se respeten el interés o los derechos y libertades fundamentales del interesado".

En la segunda sección del capítulo segundo encontramos disposiciones establecidas para considerar lícito el tratamiento de determinadas categorías de datos de carácter personal. Con respecto a los datos considerados sensibles por otras legislaciones, la primera parte del artículo 8º de la ley establece la prohibición de su recolección cuando esos datos revelen, directa o indirectamente, los orígenes raciales o étnicos, las opiniones políticas, filosóficas o religiosas o la pertenencia sindical de las personas, o que sean relativos a su salud o a su vida sexual. La segunda parte del artículo comentado atenúa la prohibición estableciendo excepciones.

El capítulo tercero de la vigente ley se ocupa de la Comisión Nacional de Informática y libertades (CNIL), de su composición y funciones (arts. 6º al 13º de la ley). Su creación se ordena por el art. 6º de la citada ley n° 78-17 en su texto original. Cuenta con potestad reglamentaria en determinados supuestos y está encargada de velar por la observancia de la legislación de protección de datos, en especial informando a las personas interesadas acerca de sus derechos y obligaciones.

La CNIL es una autoridad administrativa independiente, integrada por 16 miembros nombrados por cinco años. Además, forma parte de la Comisión un delegado del Gobierno designado por el Primer Ministro. La Comisión puede requerir a los Presidentes de los Tribunales de apelación, o a los Presidentes de los Tribunales en lo Contencioso Administrativo, a que deleguen en un juez dependiente de los mismos para llevar a cabo, bajo su dirección, misiones de investigación y control.

Todo afectado puede acudir directamente a la CNIL que pone a disposición del público la lista de los ficheros declarados ante ella. Además, la CNIL debe

presentar un informe de actividad anual al Presidente de la República y al Parlamento.

El artículo 11º de la ley vigente, textualmente concibe a la CNIL como una "autoridad administrativa independiente", y le encomienda las siguientes funciones: 1°. Informará a todos los interesados y responsables de tratamientos acerca de sus derechos y obligaciones; 2°. Velará por que los tratamientos de datos de carácter personal sean realizados de conformidad con lo dispuesto en la presente Ley. Luego, en el mismo artículo, le otorga determinadas facultades para alcanzar los objetivos antes mencionados: a) Autorizará los tratamientos mencionados en el artículo 25 (datos de carácter político, filosófico, salud y vida sexual; datos genéticos; infracciones; exclusión de un derecho; interconexiones, Número de Inscripción en el Registro; dificultades sociales; biometría), emitirá su opinión sobre los tratamientos mencionados en el artículo 26 (tratamientos de los datos sobre el Estado, la seguridad y las infracciones penales) y 27 (tratamientos públicos como el número de Inscripción en el Registro – biometría Estado – censo –tele-servicios) y admitirá las declaraciones relativas a los demás tratamientos; b) Establecerá y publicará las normas mencionadas en el punto I del artículo 24 (normas simplificadas)y promulgará, en su caso, los reglamentos tipo con vistas a garantizar la seguridad de los sistemas; c) Acogerá las reclamaciones, peticiones y denuncias relativas a la realización de los tratamientos de datos de carácter personal e informará a sus autores del seguimiento de las mismas; d) Responderá a las solicitudes de dictamen de los poderes públicos y, en su caso, de los órganos jurisdiccionales, y asesorará a las personas y organismos que realicen o tengan intención de realizar tratamientos automatizados de datos de carácter personal; e) Informará sin demora al Fiscal de la República, de conformidad con el artículo 40 del Código de Proceso Penal francés, acerca de las infracciones de las que tuviera conocimiento, y podrá presentar observaciones en el marco de los procedimientos penales, en las condiciones previstas en al artículo 52 (observaciones remitidas o presentadas por el Presidente o su representante); f) Mediante decisión expresa, podrá encargar a uno o a varios de sus miembros o agentes de sus servicios, en las

condiciones previstas en el artículo 44 (control *in situ*), la realización de comprobaciones relativas a todo tipo de tratamientos y, en su caso, obtener copias de todos los documentos o soportes de información que juzgue necesarios para ejercer sus funciones; g) En las condiciones definidas en al capítulo VII (sanciones), podrá adoptar respecto del responsable de un tratamiento, alguna de las medidas previstas en el artículo 45 (sanciones y medidas urgentes); h) Dará respuesta a las peticiones de acceso relativas a los tratamientos mencionados en el artículo 41 (tratamientos que afectan la seguridad del Estado, la defensa o la seguridad pública) y 42 (tratamientos públicos relativos a las infracciones y a los impuestos); 3°. A petición de organizaciones profesionales o instituciones que agrupen principalmente a responsables de tratamientos: a) Emitirá su opinión sobre la conformidad con las disposiciones de la presente Ley de los proyectos de normas profesionales y de los productos y procedimientos destinados a la protección de las personas respecto del tratamiento de datos de carácter personal o a la disociación de dichos datos, que le sean sometidos; b) Valorará las garantías que presentan las normas profesionales que anteriormente hubiera reconocido conforme a las disposiciones de la presente Ley en materia de respeto de los derechos fundamentales de las personas; c) Concederá un certificado a los productos o procedimientos que permitan la protección de las personas respecto del tratamiento de datos de carácter personal, una vez reconocidos estos conforme a las disposiciones de la presente Ley;4°. Se mantendrá informada de la evolución de las tecnologías de la información y publicará, en su caso, una evaluación de las consecuencias derivadas de estas para el ejercicio de los derechos y libertades mencionados en el artículo Iº (derechos humanos, intimidad de las personas, libertades individuales o públicas).

Luego la ley prescribe que para alcanzar este objetivo La Comisión Nacional de Informática y Libertades: a) Será consultada sobre todo proyecto de Ley o de decreto relativo a la protección de las personas respecto de los tratamientos automatizados; b) Propondrá al Gobierno las medidas legales o reglamentarias de adaptación de la protección de las libertades a la evolución de los procesos y técnicas informáticos; c) A petición de otras autoridades administrativas

independientes, podrá aportar su ayuda en materia de protección de datos; d) Podrá participar, a petición del Primer Ministro, en la preparación y definición de la postura francesa en las negociaciones internacionales en el marco de la protección de datos de carácter personal. Podrá participar, a petición del Primer Ministro, en la representación francesa ante las organizaciones internacionales y comunitarias competentes en esta materia. Para el cumplimiento de sus funciones, la Comisión podrá realizar recomendaciones y tomar decisiones individuales o reglamentarias en los casos previstos en la presente Ley.

La Comisión presenta cada año al Presidente de la República, al Primer ministro y al Parlamento, un informe público en el que da cuenta del cumplimiento de sus funciones.

En la ley francesa que comentamos queda muy clara la voluntad del legislador de dotar al organismo de control y aplicación de la ley, en este caso La Comisión Nacional de Libertades e Informática, de autonomía e independencia o autarquía económica para cumplir con sus funciones. Así, en el artículo 12, textualmente se ordena: *La Comisión Nacional de Informática y Libertades dispondrá de los créditos necesarios para el cumplimiento de sus funciones.*

Otro punto de interés es la composición de la CNIL, la cual queda establecida en el art. 13, de donde se desprende que se integra de forma plural por diecisiete miembros: 1º. Dos diputados y dos senadores, designados respectivamente por la Asamblea Nacional y por el Senado; 2°. Dos miembros del Consejo Económico y Social, elegidos por esta asamblea; 3°. Dos miembros o antiguos miembros del Consejo de Estado, de un grado al menos igual al de consejero, elegidos por la asamblea general del Consejo de Estado; 4°. Dos miembros o antiguos miembros de la Corte de Casación, de un grado al menos igual al de consejero, elegidos por la asamblea general de la Corte de Casación; 5°. Dos miembros o antiguos miembros de la *Cour des Comptes*[258], de un grado al menos igual al de consejero maestro,

[258] Fci: véase el sitio web oficial de la *Cour des Comptes* (Tribunal de Cuentas): http://www.ccomptes.fr/. La *Cour des Comptes* o Tribunal de Cuentas francés es el principal

elegidos por la Asamblea General de la *Cour des Comptes*; 6°. Tres personalidades cualificadas por sus conocimientos en informática o en cuestiones relativas a las libertades individuales, designadas por decreto; 7°. Dos personalidades cualificadas por sus conocimientos en informática, designadas respectivamente por el Presidente de la Asamblea Nacional y por el Presidente del Senado. La Comisión elegirá en su seno a un Presidente y a dos Vicepresidentes, entre los cuales un Vicepresidente delegado. Estos integrarán la mesa. El órgano restringido de la Comisión se compone del Presidente, de los Vicepresidentes y de tres miembros elegidos por la Comisión en su seno por la duración de su mandato. En caso de empate en la votación, el Presidente tendrá voto de calidad.

La independencia de la Comisión fue expresada por el legislador en el art. 14º, punto I, del cual se desprende que *la calidad de miembro de la Comisión será incompatible con la de miembro del Gobierno*. En igual sentido, la ley impide que los miembros de la CNIL participen en una deliberación o realicen comprobaciones relativas a un organismo en el que posean intereses directos o indirectos, o ejerzan alguna función o mandato. Tampoco pueden participar en una deliberación o realizar comprobaciones relativas a un organismo en el que hayan poseído un interés, directo o indirecto, o ejercido alguna función o mandato, en el transcurso de los treinta y seis meses anteriores a la deliberación o a las comprobaciones.

Todo miembro de la Comisión debe informar al Presidente de los intereses directos o indirectos que posee o fuera a poseer, de las funciones que ejerce o fuera a ejercer y de los mandatos que tenga o fuera a tener en el seno de cualquier persona jurídica. Dichas informaciones, así como las relativas al Presidente, estarán a disposición de los miembros de la Comisión. El Presidente de la Comisión puede adoptar las medidas necesarias para garantizar el cumplimiento de estas obligaciones establecidas en el art. 14 de la ley.

---

responsable de controlar la regularidad de las cuentas públicas del Estado, de las instituciones públicas nacionales, de las empresas públicas, de la seguridad social y de las organizaciones privadas que son asistidas o subvencionadas por el Estado francés.

El capítulo cuarto se ocupa de las responsabilidades previas al tratamiento, enumerando los principios para recabar los datos. Establece en su art. 22 la obligación de declarar el tratamiento de datos de carácter personal ante la Comisión Nacional de Informática y Libertades, salvo las excepciones expresadas por la propia ley (por ejemplo el art. 25 relativo a los datos sensibles). La declaración incluirá el compromiso de que el tratamiento cumple con las exigencias de la Ley. Puede enviarse a la Comisión Nacional de Informática y Libertades (CNIL) por vía electrónica.

En tal sentido prohíbe la recolección de datos realizada por cualquier medio fraudulento, desleal o ilícito. Otorga el derecho de la persona a ser informada cuando se recababan sus datos y algunas características y requisitos sobre el tratamiento de los datos sensibles. Reconoce también los principios: a) de lealtad y licitud en la recogida de datos; b) del secreto profesional; c) de la exactitud de los datos; d) de finalidad y pertinencia; e) de tiempo de conservación limitado; f) de seguridad y confidencialidad.

El capítulo quinto legisla sobre las obligaciones de los responsables del tratamiento de los datos y sobre los derechos de las personas (art. 32 y ss.). Los datos de carácter personal solamente podrán ser conservados más allá del plazo previsto en el apartado 5° del artículo 6 (plazo necesario para la finalidad) cuando su tratamiento tenga fines históricos, estadísticos o científicos; la elección de los datos que se conserven con estos fines se realizará en las condiciones previstas en el artículo L. 212-4 del Código del Patrimonio. Los tratamientos cuya finalidad se limite a garantizar la conservación a largo plazo de documentos de archivos en el marco del Libro II del mismo Código, estarán dispensados de las formalidades previas a la realización de los tratamientos previstas en el capítulo IV (formalidades previas a la realización de los tratamientos) de la presente Ley.

Se podrá realizar un tratamiento cuyas finalidades sean distintas de las mencionadas en el primer párrafo con el consentimiento expreso del interesado.

La ley francesa reconoce el ejercicio del derecho de acceso, junto con los de rectificación y, en su caso, cancelación, al expresar en el art. 36 que el titular del derecho de acceso podrá exigir que las informaciones que le afectaren y fueren inexactas, incompletas, equívocas, caducadas, o cuya colecta, utilización, comunicación o conservación estuviere prohibida, sean debidamente rectificadas, completadas, aclaradas, actualizadas o canceladas. El trámite de solicitud de información registrada se realizaba a cambio del pago de una tasa variable en función del tipo de tratamiento, y cuyo importe era fijado por resolución de la Comisión y homologado por Orden del Ministro de Economía y Hacienda.

El capítulo sexto regula el control en la realización del tratamiento de los datos personales, y el séptimo determina las Sanciones que puede dictar la Comisión Nacional de Informática y Libertades. Las sanciones penales aplicables por el tratamiento ilícito de datos de carácter personal pueden encontrarse en el capítulo VIII de la ley.

El capítulo noveno se ocupa del tratamiento de datos de carácter personal con fines de investigación en el ámbito de la salud. El capítulo décimo hace lo mismo con respecto a los datos personales de salud con fines de evaluación o de análisis de las prácticas o de las actividades de asistencia y prevención sanitarias.

Los datos personales tratados con fines periodísticos y de expresión literaria y artística son regulados por el capítulo XI de la ley.

El tratamiento de datos personales sobre solvencia patrimonial y crédito sin consentimiento del afectado, está permitido en Francia sin contravención a la ley 78/17 de protección de datos, siempre y cuando se respete lo establecido en los principios generales de la mencionada ley[259].

[259] Además de los mencionados principios de la ley francesa Nº 78/17, todo tratamiento de datos personales sobre solvencia patrimonial y crédito debe respetar los siguientes artículos de esa misma norma: 3, 25, 26, 29, 34 y 37.

Finalmente la transferencia de datos de carácter personal hacia Estados que no pertenecen a la Comunidad Europea se encuentra regulada en el capítulo XII de la ley francesa.

9.- Grecia

La Constitución de la República Helénica reconoce el derecho de toda persona a la privacidad y a la confidencialidad de las comunicaciones. La Carta Magna griega expresa textualmente en el artículo 9°: "la casa de cada persona es inviolable; es un santuario de la vida privada y familiar de la persona en el que ninguna búsqueda se efectuará, a excepción de aquellas que estén amparadas por la ley en la forma, el tiempo y en presencia de representantes del poder judicial. Los infractores de la disposición anterior serán sancionados por violar el asilo de la casa y por abuso de poder, siendo responsables de los daños y perjuicios causados a la víctima, según lo especificado por la ley".

La Constitución Helénica fue reformada en el año 2001, oportunidad en la que se incorporó al artículo antes mencionado, el derecho de la persona a la protección de su información personal. Así, el reformado artículo 9 actualmente expresa: "Todas las personas tienen derecho a ser protegidas de la recolección, procesamiento y uso, especialmente por medios electrónicos, de sus datos personales, según lo especificado por la ley"; también dispone en una segunda parte que "la protección de datos está garantizada por una autoridad independiente, que se establece y opera según lo especificado por la ley".

El artículo 19 de la Constitución griega también se ocupa de la protección de la privacidad de las comunicaciones al establecer que: "El secreto de la correspondencia y de cualquier otra forma de comunicación libre es absolutamente inviolable. La autoridad judicial no se considera obligada por este secreto por razones de seguridad nacional o para el fin de investigar delitos especialmente graves que se especifiquen en la ley".

La modificación de 2001, además de agregar dos nuevas disposiciones a este artículo, establece una autoridad independiente que vigila los asuntos relacionados con las telecomunicaciones.

Con las modificaciones mencionadas, actualmente el artículo 19 (2) cuenta con el siguiente texto: "Los asuntos relacionados con el establecimiento, funcionamiento y competencias de la autoridad independiente que garantice el secreto de las telecomunicaciones se determinarán por ley". La tercera parte de este art. 19 establece que: "El uso de pruebas obtenidas en violación del presente artículo y a los artículos 9 y 9A está prohibido".

Luego de la firma del Convenio del Consejo de Europa el 17 de febrero de 1983, ratificado en agosto de 1995, la República de Helénica legisló sobre la protección de los datos personales por medio de la ley número 2472[260] de 1997, de "protección de las personas con respecto al tratamiento de los datos de carácter personal". Se trata de una ley ambiciosa cuyo ámbito de aplicación va más allá de la directiva 95/46/CE, con la claridad y transparencia que le proporciona el hecho de tener pocas excepciones[261]. Esta ley 2472 fue modificada por las leyes 2819 del año 2000 y 2915 del año 2001[262]. En el año 2006 Grecia dictó la ley Nº 3471/2006 de Protección de los datos personales y la intimidad en el sector de las telecomunicaciones electrónicas, por medio de la cual también se modifica la ley 2472/1997[263].

La Ley sobre la protección de las personas con respecto al tratamiento de Datos de Carácter Personal (LOPD), fue aprobada por el Parlamento griego en abril

[260] La ley 2472 fue aprobada el 10 de abril de 1997 y publicada el 24 de octubre de 1997; contiene 26 artículos.
[261] Revista "Privacy Laws & Business & Newsletter"; Edición de Agosto de 1997, citada por Miguel Ángel Davara Rodríguez: *La Protección de Datos en Europa Principios, derechos y procedimientos*. Editorial Grupo ASNEF-EQUIFAX – Universidad Pontificia Comillas ICAI-ICADE. Madrid, 1998, p. 150.
[262] El texto de la ley 2472 y sus modificatorias en Ingles, puede ser encontrado en el sitio web de la *Hellenic Data Protection Authority*.
Fci.: http://www.dpa.gr/legal_eng.htm.
[263] Fci: http://www.dpa.gr/portal/page?_pageid=33,43560&_dad=portal&_schema=PORTAL (última consulta el 13 de septiembre de 2011).

de 1997. Grecia fue el último miembro de la Unión Europea (UE) en adoptar una ley de protección de datos personales. Esta ley tiene como particularidad, que por la fecha en que fue sancionada, ya incorpora la Directiva de Protección de Datos (1995/46/CE) de la Unión Europea al sistema jurídico griego y a través de ella, Grecia ingresa al Acuerdo de Schengen.

A partir de la sanción de la ley de protección de datos personales, Grecia fue incorporando a su legislación nacional todas las directivas de protección de datos de la UE en el sector de las telecomunicaciones, con la excepción de la Directiva de Retención de Datos de 2006.

La primera modificación importante a la Ley de Protección de Datos de 1997 entró en vigor en el año 2006. La enmienda define el término "datos personales" y añade disposiciones relativas a la transferencia de datos a terceros países.

Una segunda modificación importante se realizó en el año 2007, como consecuencia de una disputa que tuvo lugar entre la Autoridad de Protección de Datos y la Autoridad de Policía griega, ya que esta última planeaba utilizar las cámaras de CCTV (originalmente instaladas para controlar el tráfico durante los Juegos Olímpicos de Atenas) para controlar reuniones públicas y protestas. En octubre de 2007, la Corte Suprema falló a favor del plan de la autoridad policial, pero más tarde, la Ley N º 3625/2007 que modifica la Ley de Protección de Datos fue aprobada con el fin de excluir a las cámaras de CCTV del ámbito de aplicación de la ley. En la práctica, la enmienda de 2007 era mucho más importante, ya que prácticamente ha excluido del ámbito de aplicación de la Ley de Protección de Datos a todos los datos personales relacionados con el delito de procesamiento. La enmienda, aunque inspirada por la necesidad de utilizar las instalaciones de cámaras de circuito cerrado para fines distintos de control de tráfico (es decir, durante las manifestaciones públicas), con el tiempo coloca fuera de las disposiciones de protección de datos, a todo tratamiento de datos personales realizado por las autoridades de persecución del delito cuando se realiza en el proceso de enjuiciamiento de una amplia lista de crímenes (por ejemplo, contra la vida humana

o la propiedad, delitos relacionados con drogas, delitos contra el orden público, delitos contra menores, etc.).

La actual ley griega Nº 2472 de Protección de Datos Personales está estructurada en seis capítulos. El primer capítulo, titulado "Disposiciones Generales", se desarrolla en los artículos 1, 2 y 3. Trata sobre el objeto, sobre algunas definiciones y sobre el ámbito de aplicación de la ley. Al respecto, podemos resaltar que esta ley, en el artículo 3º, alcanza tanto al "tratamiento automatizado, total o parcial, de datos de carácter personal, como al tratamiento no automatizado de datos contenidos o llamados a incluirse en un fichero".

El capítulo segundo indica las características que deben reunir los datos de carácter personal para ser objeto de lícito tratamiento (artículo 4), así como las condiciones previas para la realización del tratamiento (artículo 5) y la obligación del responsable de notificar a la autoridad de Control el establecimiento y funcionamiento del archivo (artículo 6). En este sentido, los datos deben recogerse de manera leal, lícita y honesta, con fines determinados, explícitos y legítimos. Deben ser coherentes, oportunos y no excesivos con respecto al fin del tratamiento, ser exactos, actualizados y conservarse durante un período que no rebase el tiempo necesario para alcanzar los objetivos.

El capítulo tercero reconoce a los interesados los derechos de información en la recogida de datos (art.11), de acceso y de objeción que comprende la petición para una acción específica, como por ejemplo la corrección, la no utilización con carácter provisional, el bloqueo, la no transmisión o la supresión de los datos[264](art. 13).

El derecho de acceso y el de objeción se ejercerán mediante el depósito de una suma, cuyo importe se establecerá por decisión de la Autoridad de Control, que la rembolsará al interesado si se considera fundada su petición de corrección o de supresión de los datos.

[264] Véase el art. 13 de la ley 2472 de Protección de Datos (Grecia).

En cuanto al incumplimiento por el titular del fichero de los principios de protección de datos recogidos en la ley, el capítulo quinto contempla dos tipos de sanciones: administrativas o penales.

Las sanciones administrativas (art. 21º) son impuestas por la Autoridad Helénica de Protección de Datos y pueden consistir en una advertencia, acompañada de un plazo para hacer la transgresión, multa; cese provisional o definitivo de la autorización para funcionar, la destrucción del archivo de datos o la interrupción del tratamiento y destrucción de los datos en cuestión.

Las sanciones penales llegan a una pena de tres años de prisión cuando se omita alguna de las garantías previstas en la ley para el tratamiento de los denominados "datos sensibles", o cuando se proceda a interconectar ficheros sin notificarlo a la Autoridad de Control, además de otras múltiples acciones dolosas que figuran en el artículo 22 y que pueden llevar el máximo de diez años de reclusión cuando el que incumpliere, demás tuviera la intención de "sacar para sí mismo o para un tercero beneficio financiero legal".

La Autoridad de Protección de Datos Helénica (*Hellenic Personal Data Protection Authority*)[265], es la autoridad de control constituida por la ley de protección de datos, que se encuentra regulada en el capítulo IV de la ley, con el título de autoridad de control protectora de datos de carácter personal[266].

Esta autoridad se crea con el objeto de vigilar la aplicación de la ley de protección de datos y de lograr que los tratamientos de datos personales no lesionen los derechos de las personas. Destaca la precisión y la amplitud con la que se han desarrollado las funciones y obligaciones de esta autoridad, a la que se le reconocen, entre otros poderes, potestad normativa, inspectora y sancionadora. Cuenta con el apoyo de una Secretaría formada por un número no superior a treinta funcionarios (art. 20º).

---

[265] Autoridad Helénica de Protección de Datos (*Hellenic Data Protection Authority*). Fci.: http://www.dpa.gr/legal_eng.htm .

[266] Sobre esta Autoridad de Control ver los artículos 15-23 de la Ley griega.

Se constituye como una autoridad pública e independiente que no estará sometida a ningún control administrativo y cuyos miembros disfrutarán de independencia personal y profesional en el ejercicio de sus funciones, que se centran en la vigilancia de la aplicación de la ley griega de protección de datos personales.

La Autoridad de Control está integrada por un magistrado que ocupará el cargo de Presidente, un profesor de un centro de enseñanza superior especializado en Derecho y otro especializado en Tecnologías de la Información, además de tres personas con experiencia en el ámbito de la protección de datos de carácter personal.

El mandato de sus miembros será de cuatro años pudiendo ser reelegidos por un nuevo período. Entre las competencias de la Autoridad de Control cabe destacar la emisión de directivas orientadas a la interpretación de la ley así como de recomendaciones y sugerencias a los responsables del tratamiento, extendiendo las autorizaciones previstas en la norma y denunciando a las autoridades competentes las transgresiones a sus disposiciones.

La Autoridad de Control tiene potestad inspectora y sancionadora, así como reglamentaria para resolver cuestiones particulares, técnicas y de detalle "a las cuales se refiera la ley". Entre sus funciones se encuentra la de llevar el registro de los archivos y tratamiento, la de autorizar transferencias e interconexiones y asistir a las personas que no deseen figurar inscriptas en ficheros cuyo objetivo sea la promoción comercial o la oferta de productos por correspondencia.

A partir de la entrada en vigor de la ley, la autorización del tratamiento quedó condicionada a su articulado. La ley permite el tratamiento de datos personales sobre el cumplimiento o incumplimiento de obligaciones dinerarias sin consentimiento del interesado, con base en la excepción prevista en el apartado 2 a) del artículo 5, que indica que autorizará el procesamiento de datos sin consentimiento del afectado cuando "el tratamiento resulte necesario para cumplir

con obligaciones derivadas de un contrato del cual el interesado forme parte o para cumplir con medidas precontractuales tomadas a petición del interesado" o, también en la interpretación que se pueda dar en este sentido a lo expresado en el apartado 2 e), del mismo artículo, que permite el tratamiento sin consentimiento cuando sea absolutamente necesario para "conseguir el interés legítimo pretendido por el responsable del tratamiento o por el o los terceros en cuyo conocimiento se pongan los datos y con la condición de que dicho interés sea manifiestamente superior a los derechos e intereses de las personas a las cuales se refieran los datos, y en la medida en que sus libertades fundamentales no resulten vulneradas".

10.- Holanda

Luego de ratificar el Convenio del Consejo de Europa el 24 de agosto de 1993, que entró en vigor el 1 de diciembre del mismo año, Holanda modificó su legislación sobre la protección de datos personales el 23 de noviembre de 1999, en su sesión Nº 92 del período parlamentario 1999 - 2000 mediante la ley 25.892 de Protección de Datos Personales (*Wetbescherming Persoonsgegevens*)[267] con el objetivo de adecuar su legislación a la Directiva Europea 95/46/CE.

La ley holandesa de protección de datos personales se aplica tanto a los archivos del sector público como a los del sector privado y a los automatizados como a los manuales, cuando estos últimos poseen una estructura lógica que permita una consulta metódica de sus datos. Como ya dijimos, esta norma vino a modificar la anterior ley holandesa de protección de datos personales de 1988, conocida como WPR *(Wetpersoneneregistraties)*[268].

Se exige para la creación y mantenimiento de un archivo de titularidad pública un reglamento sobre el funcionamiento del tratamiento que se va a realizar y una declaración ante la autoridad de control denominada *College Bescherming*

[267] Se puede encontrar el texto completo de esta ley, tanto en su idioma original como traducida al inglés en el sitio web de la CBP (http://www.cbpweb.nl).
[268] Davara Rodríguez. M. (1998). Op. cit., p. 154.

Persoonsgegevens (CBP)[269], a fin de que pueda ser consultado por cualquier interesado. Diferente es el trámite para los archivos del sector privado, ya que la declaración de los tratamientos se efectúa en un formulario, indicando las principales características.

Dentro del Capítulo Primero de "Provisiones Generales", el artículo primero enuncia una lista de definiciones, que principian con el concepto de dato personal, al cual la ley define como "cualquier información relativa a una persona natural identificada o identificable". Observamos que este concepto no alcanza a los datos personales de las personas ideales o jurídicas, las cuales quedan fuera del alcance de la ley.

La ley enuncia en el Capítulo Segundo, los principios de: licitud para recabar datos, exactitud de los mismos, pertinencia y proporcionalidad con el fin, confidencialidad, seguridad y tiempo de conservación limitada. Reconoce a los afectados el derecho de obtener información previa por escrito sobre el primer registro en el mes siguiente a su inclusión en el archivo, el derecho de acceso a la información que les concierne en el mes siguiente a su petición el derecho de rectificación y/o cancelación en un tiempo de dos meses a contar desde la petición y el derecho a ser informados, bajo petición, sobre la comunicación de sus datos a terceros.

Existen excepciones al derecho de acceso relacionadas con la seguridad del Estado, un interés económico y financiero del Estado o de los organismos públicos, así como en las investigaciones administrativas o judiciales.

La autoridad de control holandesa, el *College Bescherming Persoonsgegevens*, es también conocida como Cámara de Registro o Comisión de Protección de Datos cuya composición y funciones se encuentran reguladas en el

[269] *College Bescherming Persoonsgegevens* es el nombre de la autoridad de control holandesa en materia de Protección de Datos Personales. Fci.: su sitio web se encuentra en la siguiente dirección: http://www.cbpweb.nl (último ingreso el 18/9/2012).

capítulo 9 (arts. 51 en adelante) de la nueva ley holandesa de protección de datos[270].

La Comisión de Protección de Datos constituye un órgano administrativo independiente compuesto por un presidente y dos miembros, encargado de velar por la aplicación y cumplimiento de la ley. La Comisión puede designar a miembros especiales, para reflejar la variada composición de la sociedad holandesa[271]. El presidente es designado por seis años, mientras los otros miembros, junto con los miembros especiales, lo son por cuatro años. Todos ellos son designados por Real Decreto. El presidente no puede ejercer ninguna otra función remunerada sin autorización del Ministro de Justicia.

La Autoridad de Control busca reflejar una composición acorde con el entorno económico. Dispone de potestad investigadora, ya sea de oficio o a petición de parte, y tiene poder para obtener toda información o documento necesario para realizar sus funciones. Emite informes a petición de un tribunal encargado de decidir sobre un conflicto relativo a la protección de datos y controla la realización e implantación de los códigos de buena conducta, resultado de la autoregulación de los diferentes sectores.

Cada año debe enviar al Ministro de Justicia un informe sobre su actividad.

Toda persona que se considere lesionada puede acudir a la Cámara de Registro y solicitar gratuitamente que realice el papel de intermediario. En caso de litigio con el responsable del fichero, el interesado puede también acudir al Tribunal de Gran Instancia competente, que condenará en el caso concreto al pago de daños y perjuicios.

Las sanciones penales se encuentran reguladas a partir del artículo 75 y siguientes. La falta de declaración constituye un delito penado con multas o con prisión de una duración de seis meses.

[270] La ley holandesa también puede ser encontrada en una traducción al inglés, disponible en el sitio web http://home.planet.nl/~privacy1/wbp.htm).
[271] Artículo 53 de la nueva ley holandesa de protección de datos personales.

La ley holandesa de datos no contiene reglas específicas sobre la posibilidad de creación de ficheros sobre cumplimiento o incumplimiento de obligaciones dinerarias sin consentimiento del afectado.

11.- Irlanda

La República de Irlanda firmó el Convenio del Consejo de Europa, luego ratificado el 25 de abril de 1990, que entró en vigor el 1 de agosto del mismo año. La legislación nacional de Irlanda dictó la ley de protección de datos personales el 13 de julio de 1988[272], que entró en vigor el 19 de abril de 1989 y que fijó como objetivo la aplicación del acuerdo del Consejo de Europa e incluso el texto del convenio fue incorporado al texto de la ley como anexo. En el año 2003 Irlanda modificó la ley de 1988 para adaptar su legislación a la Directiva 95/46/CE. También se incorporó a la legislación irlandesa el Reglamento de la Privacidad Electrónica en el año 2011 (SI 336 de 2011) para regular la protección de datos de teléfono, e-mail, SMS y el uso de Internet. Este reglamento busca adaptar la legislación de Protección de Datos irlandesa a la Directiva de la UE 2002/58/CE (modificada por la Directiva 2006/24/CE y 2009/136/CE).

La primera sección de la ley de 1988 se refiere a su interpretación y aplicación. A tal efecto, comienza con un listado de definiciones y conceptos relacionados con su contenido. Define al dato personal expresando que son los datos de las personas individuales vivas, que pueden ser identificadas tanto a partir de una información personal como de un conjunto de datos con otras informaciones en posesión del usuario o recolector de datos. Como se observará, esta ley[273] no incluye, en su concepto de dato personal, a los datos de las personas ideales o jurídicas, dejándolas al margen de su protección[274].

[272] La ley irlandesa de Protección de Datos de 1988 puede ser consultada, en lengua inglés, en el sitio web http://www.dataprivacy.ie/6ai.htm (última visita el 15 de diciembre de 2011).
[273] En igual sentido lo hace la ley holandesa de protección de datos personales.
[274] Textualmente la ley establece el concepto de dato personal, expresando: "*personal data" means data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller*".

La segunda sección de la ley[275] se centra en la recolección de datos, registro, tratamiento y transferencia de los datos, que deben ser realizados con un propósito lícito y bajo ciertos principios de lealtad, exactitud, actualización, proporcionalidad y adecuación al fin o propósito. Su conservación se permite sólo durante un tiempo, acorde con el fin y seguridad y confidencialidad.

La tercera Sección de la ley[276] garantiza el derecho a conocer la existencia de datos personales en no más de 21 días siguientes a la solicitud y gratuitamente[277].

Esta ley de protección de datos se aplica tanto al sector público como al privado, exclusivamente a archivos automatizados y, como ya dijimos, solamente a las personas físicas. Siguiendo los lineamientos del derecho comparado, no forman parte de su ámbito de aplicación los datos relativos a las agencias de inteligencia y de seguridad nacional. Tampoco integran su ámbito de aplicación aquellos datos que sean considerados de acceso público en virtud de una ley que así lo establezca y los datos personales conservados con un objetivo exclusivamente familiar y personal.

Encontramos que la ley irlandesa ha seguido un sistema de inscripción y registro[278] de archivos de tipo "selectivo", dado que la inscripción sólo es obligatoria para los archivos del sector público y aquellos del sector privado pertenecientes a instituciones financieras, compañías de seguros, empresas de venta por correo y empresas que prestan información en materia de crédito. También deben registrarse aquellos bancos de datos específicamente indicados por procesar datos de carácter sensible sobre origen racial, opiniones políticas o religiosas u otras creencias, salud física o mental, vida sexual o condenas criminales.

---

[275] La Segunda Sección de la ley se titula: "*Protection of Privacy of Individuals with regard to Personal Data Collection, processing, keeping, use and disclosure of personal data*".
[276] La Tercera Sección, lleva por título: *Right to establish existence of personal data.*
[277] Miguel Ángel Davara explica que el derecho a conocer los datos personales se complementa con un "*derecho de acceso que incluye el envío de una copia de los datos pagando una determinada cantidad, junto al derecho de exigir la rectificación o cancelación de los datos inexactos o registrados indebidamente y el de hacer retirar el nombre de las listas de mailing".* Ver: Davara Rodríguez, M. (1998). Op. cit., p. 161.
[278] Sección 16 (*The Register)* de la *Data Protection Act* irlandesa de 1988.

La registración habilita al funcionamiento lícito del banco de datos por un período de tiempo que prescribe una vez cumplido y obliga a su titular a removerlo. El período mínimo es de un año.

El derecho de acceso[279] se encuentra legislado en la sección Nº 4 de la ley de protección de datos, y en la sección siguiente (Nº 5) se regula la restricción al derecho de acceso[280]. En esta quinta sección se establecen excepciones al derecho de acceso, cuando se trata de datos relativos a prevención de delitos, fraude fiscal, relaciones internacionales, seguridad pública, secreto profesional y a funciones de investigación o relacionadas con las estadísticas.

Cuando se considere que puede haberse causado un daño como consecuencia del tratamiento automatizado de los datos de carácter personal, la ley prevé que se pueda acudir a una acción de daños y perjuicios.

Al igual que la ley inglesa, la irlandesa basa su regulación en el registro de los ficheros aunque lo realice de una forma selectiva, teniendo en común también con la británica el aliento e impulso que se quiere proporcionar a la elaboración de códigos de conductas que como adelante indicamos, en el caso de la ley irlandesa puede llegar a adquirir el carácter de normas reglamentarias.

La Oficina del Comisionado de Protección de Datos es un organismo independiente establecido por la ley de protección de datos de 1988, en su sección IX, como autoridad de control en Irlanda (*Data Protection Commissioner*[281]).

El Comisionado nombrado por el Gobierno por un período de cinco años, es independiente en el ejercicio de sus funciones y goza de personalidad jurídica propia. Vela por la aplicación de la ley y no puede ejercer ninguna otra actividad remunerada.

---

[279] Sección 4, *The right of access*
[280] Sección 5, (*Restriction of right of access*) de la ley de protección de datos personales.
[281] Comisionado de Protección de Datos de Irlanda. Fci.: http://www.dataprivacy.ie/ (última visita el 15 de Diciembre de 2011).

Puede investigar a los titulares de ficheros, tanto de oficio como a instancia de parte, teniendo la facultad de solicitar que se proceda a la cancelación o ratificación de datos. Todas sus resoluciones o acciones que incidan sobre un comportamiento de un titular de un archivo, pueden ser apeladas ante los tribunales.

Debe impulsar a las asociaciones u organizaciones de carácter profesional a la realización o elaboración de códigos de conducta que se someten a su aprobación, al tiempo que pueden ser remitidos por el Ministerio de Justicia al Parlamento y, si son aprobados por éste, adquieren rango de ley.

El Comisionado para la protección de datos tiene obligación de remitir un informe anual al Parlamento. Tiene potestad inspectora, pudiendo entrar en las instalaciones en las que se encuentren ficheros automatizados de datos de carácter personal y se presuma que tengan una actuación irregular, registrándolos y requiriendo a las personas que en ellos trabajen que le entreguen la documentación que necesite en la inspección y que le faciliten los datos necesarios para su realización. No obstante, para poder ejercer esta función y entrar en los locales de las instituciones financieras, el Comisario necesita un mandamiento u orden que le debe proporcionar el Tribunal Superior Irlandés.

La ley irlandesa de protección de datos de 1988 tiene gran similitud con la ley británica, sobre todo en los principios de protección de datos y no prohíbe de forma expresa la recolección o el tratamiento de datos personales sobre solvencia patrimonial y crédito sin consentimiento del afectado. Y en la práctica, el tratamiento y el uso de datos personales sobre solvencia patrimonial, y crédito está muy extendido en Irlanda[282].

No obstante, es importante señalar que su artículo 2 (1) recoge un principio muy similar al primer principio de protección de datos de la ley británica: “el responsable del tratamiento deberá, con respecto a los datos personales tratados por

[282] Davara Rodríguez, M. (1998). Op. cit., p. 164.

él, cumplir con las siguientes reglas: a) los datos o en su caso, la información de la que los datos se derivan, ha de ser obtenida y los datos han de ser tratados de forma leal".

Este artículo puede ser interpretado de la misma forma que el primer principio de protección de datos ha sido interpretado para la ley británica.

El artículo 16 (1) b) de la ley de protección de datos irlandesa requiere que "las personas cuyo negocio consista total o parcialmente en la provisión de información sobre crédito" deberán hacerse registrar en el registro del Comisario de Protección de Datos (*Data Protection Commissioner*). Esta autoridad mantiene un registro público de todos los tratamientos de datos personales que, según la ley irlandesa, han de ser registrados.

12.- Italia

Luego de ratificar el Convenio del Consejo de Europa firmado el 2 de Febrero de 1983, la República de Italia aprobó su ley de protección de datos personales[283] con el Nº 675/96 de 31 de diciembre de 1996 (publicada en el Boletín Oficial de 8 de enero de 1997) luego modificada en mayo y julio de 1997 por las leyes 123/97 y 255/97, respectivamente.

Al igual que la legislación griega, esta ley italiana fue una de las últimas leyes europeas de protección de datos en dictarse. Entró en vigor el 8 de mayo de 1997 y su más reciente modificación fue realizada por la ley 467 del 28 de diciembre del año 2001. Esta ley contiene en su articulado a todos los principios y derechos en materia de protección de datos. Siguiendo la técnica legislativa europea, comienza con un capítulo primero de *Principios Generales*[284], donde

[283] La ley Italiana Nº 675 de Protección de la Persona en el Tratamiento de sus Datos Personales (*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* (texto consolidado el 28 de diciembre de 2001, n. 467*)*.Su texto completo (en inglés e Italiano) puede ser consultado en la siguiente fci.: http://www.garanteprivacy.it/garante/frontdoor/1,1003,00.html?LANG=1**.**

[284] Cattaruzza, A.; Galbiati, R.; Panieri, B., y Zampetti, A. *La tutela dei dati personali*. 2º ed. Ed. Buffetti Editori Multimedia. Grupo Buffetti. Roma, 1998, p.185.

plasma conceptos y definiciones a los efectos de su interpretación. En el artículo 1º, apartado 2º, inc. c) define al Dato Personal, expresando que es "*cualquier información relativa a las personas naturales o jurídicas, entes o asociaciones que sean identificadas o identificables en forma directa o indirectamente por referencia a cualquier otra información, incluyendo los números de identificación personal"*. Podemos destacar en la ley italiana, que, en sintonía con la doctrina de su tiempo, extendió su protección no solo a las personas físicas, sino también a las personas jurídicas.

En cuanto al incumplimiento por parte del titular del banco de datos, de los principios y derechos de protección de datos, la ley establece sanciones administrativas en su artículo 39[285], con importantes multas y penas de privación de libertad para aquellas acciones que tipifica como constitutivas de delitos, con base en principios de incriminación de conductas dolosas.

El artículo 30 de la ley italiana de protección de datos crea la institución del *Garante per la Protezione dei Dati Personali*[286] y establece sus competencias. Es un órgano colegiado, autónomo, independiente, que se compone de cuatro miembros, elegidos por la Cámara de diputados y senadores de la República. El Garante dispone de un presidente que es elegido dentro del ámbito del cuerpo colegiado, y cuyo voto prevalece en caso de empate. El presidente dura cuatro años, y no puede ser reelegido. Los miembros de esta institución deben ser personas de reconocida independencia y experiencia en el campo del derecho, de la informática y de las nuevas tecnologías de la información.

La ley italiana de protección de datos autoriza la incorporación de datos personales en los archivos de información patrimonial y solvencia económica, sin consentimiento del afectado[287]. Tal autorización surge del artículo 12, 1 b) de la

[285] El órgano competente para recibir el informe y aplicar la sanción es el Garante para la Protección del Dato Personal (art. 39, inc. 3 de la ley 675).
[286] El sitio web oficial de la autoridad de control italiana (*Garante per la Protezione dei Dati Personali),* es el siguiente fci.*: http://www.garanteprivacy.it*; (última consulta el 15 de Diciembre de 2011).
[287] Davara Rodríguez, M. (1998). Op. cit., p. 165.

ley, que permite el tratamiento de datos personales sin consentimiento del afectado cuando el procesamiento de tales datos sea necesario para la ejecución de las obligaciones contractuales en las que el interesado sea parte. Además, el artículo 12, 1 f) de la ley destaca el hecho de que el consentimiento del afectado no es necesario cuando el tratamiento de datos personales concierne a actividades económicas.

El artículo 20 de la ley italiana está dedicado a los requisitos para la comunicación y difusión de datos personales. El primer apartado de este artículo afirma que dicha comunicación o difusión solo podrá tener lugar en los siguientes casos: a) Con el consentimiento expreso del interesado; b) Cuando se trate de datos provenientes de fuentes accesibles al público (registros públicos, actos o documentos cuya publicidad haya sido reconocida por la ley); c) Cuando se trata de datos relativos al desarrollo de actividades económicas, con respecto a la normativa vigente en materia de secreto bancario e industrial.

13.- Portugal

A partir del artículo 35[288] de su Constitución Nacional de 1976, Portugal legisló sobre la protección de los datos personales el 9 de abril de 1991 mediante la ley 10/91 de "protección de datos personales frente a la informática". Esta norma omitió establecer en forma expresa las condiciones de licitud para el procesamiento

[288] El artículo 35 de la Constitución de Portugal de 1976 textualmente expresa:
l) - Todos los ciudadanos tienen derecho de acceso a sus datos informatizados, pudiendo exigir su rectificación y actualización o el derecho a conocer la finalidad a la que se destinan en los términos de la ley. 2) – Una ley definirá el concepto de datos personales así como las condiciones aplicables para su tratamiento automatizado, conexión, transmisión y utilización, y garantizará su protección a través de una entidad administrativa independiente. 3) - La informática no puede ser utilizada para el tratamiento de datos referentes a convicciones filosóficas o políticas, filiación partidaria o sindical, fe religiosa, vida privada y origen étnico, salvo mediante consentimiento expreso del titular, autorización prevista por ley como garantía de no discriminación o para procesamiento de datos estadísticos no individualmente identificables. 4) – Está prohibido el acceso a datos personales de terceros, salvo en casos excepcionales previstos en la ley. 5) – Queda prohibida la atribución de un número único de identificación nacional a los ciudadanos. 6) – Se garantiza el libre acceso a las redes informáticas de uso público, definiendo una ley o régimen aplicable al flujo de datos transfrontera y a las formas adecuadas de protección de datos personales en otros países cuya salvaguarda se justifique por razones de interés nacional. 7) – Los datos personales constantes de archivos manuales gozan de protección idéntica a la prevista en los incisos anteriores y en los términos de la ley.

de datos personales; tampoco exigió el consentimiento del afectado para poder tratar sus datos personales[289]. Posteriormente, el 2 de septiembre de 1993 Portugal ratificó el Convenio del Consejo de Europa, que entró en vigor el 1 de enero de 1994 y a partir del cual se aprobó la ley 28/94 del 29 de agosto de 1994 que vino a incorporar medidas de refuerzo a la protección de datos personales en ya mencionada la ley 10/91.

Posteriormente, Portugal, obligado por las directivas europeas 95/46/CE y 97/66/CE, derogó sus leyes de protección de datos personales 10/91 y 28/94 para poner en vigencia la ley 67/98[290] (que vino a transponer al derecho interno portugués la directiva 95/46/CE). También sancionó las leyes 68/98 y 69/98, esta última a los efectos de transponer a su derecho interno la Directiva 97/66/CE, relacionada con la protección de datos personales en el sector de las telecomunicaciones.

En su segundo artículo, la ley 67/98 enuncia un principio general, según el cual "el tratamiento de los datos personales debe procesarse de forma transparente y en un estricto respeto por la reserva de la vida privada, así como los derechos, libertades y garantías fundamentales". Este punto de partida de la ley portuguesa es altamente positivo, dado que marca una línea rectora de interpretación y aplicación de los preceptos siguientes de la norma.

El artículo 3º define conceptos y términos a los efectos de la interpretación y aplicación de la ley 67/98 de protección de datos personales. Entre ellos se destaca la definición de datos personales, respecto de los cuales expresa que son "cualquier información de cualquier naturaleza e independientemente de su respectivo soporte, incluidos sonido e imagen, relativa a una persona física[291], identificada o identificable (titular de datos); se considera identificable a una persona que pueda

[289] Davara Rodríguez, M. (1998). Op. cit., p.170 y siguientes.
[290] Legislación portuguesa sobre protección de datos personales.
Fci: http://www.cnpd.pt/Leis/leis.htm .
[291] La ley en su idioma original usa las palabras *pessoa singular, identificada ou identificábel,* a lo que podemos traducir por "persona física, identificada o identificable", por considerar que de esta forma se llega a una traducción más exacta en su contexto.

ser identificada directa o indirectamente, designada por referencia a un número de identificación o a uno o más elementos específicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Relacionando el artículo 1º (Objeto) y el artículo 4º de la ley 67/98, surge que el ámbito de aplicación de esta ley de protección de datos personales alcanza a los archivos de datos personales tanto del sector público como a los del sector privado y excluye de la ley a los datos de las personas jurídicas. Regula a los bancos de datos total o parcialmente automatizados, así como a aquellos que procesen información por medios no automatizados de datos personales contenidos en ficheros manuales[292].

Los bancos o archivos de datos tienen permitido el tratamiento, sean públicos o privados, cuando no contienen datos sensibles[293]. Están obligados a informar a la autoridad de control sobre la creación del banco de datos mediante una comunicación detallada sobre el contenido de los datos. A *contrario sensu*, la ley establece la prohibición del tratamiento de datos personales sensibles, referentes a convicciones filosóficas o políticas, filiación partidaria o sindical, fe religiosa, vida privada y origen étnico, así como el tratamiento de datos relativos a salud y vida sexual, incluidos los datos genéticos. Esta prohibición, como regla general, tiene una serie de excepciones en el mismo artículo 7º de la ley 67/98, entre las que se destacan motivos de interés público, de medicina preventiva y otros taxativamente enumerados por el artículo mencionado.

La legislación portuguesa sólo permite recoger datos personales tratados en forma lícita y con respeto al principio de buena fe, recogidos para finalidades determinadas, explícitas y legítimas, que sean relevantes, pertinentes y adecuados para la finalidad del procesamiento de datos autorizado por la autoridad de

[292] Artículo 4º inc. 1º de la ley 67/98.
[293] Artículo 7 de la ley 67/98.

aplicación[294]. Con respecto a la calidad de los datos, se exige que los datos sean exactos, correctos y actualizados[295].

La ley establece que "el responsable del tratamiento de datos de un archivo o banco de datos, está obligado a poner en práctica las medidas técnicas y organizativas adecuadas para proteger los datos personales contra la destrucción accidental o ilícita, la pérdida accidental o la alteración y difusión o acceso no autorizado, particularmente cuando el tratamiento implique su transmisión por red o contra cualquier otra forma de tratamiento ilícito"[296]. A su vez, vemos que el artículo 17º de la ley 67/98 obliga al responsable del banco de datos, así como a las personas que en ejercicio de su funciones tengan conocimiento de los datos personales tratados, a mantener en todo momento, aun una vez concluidas sus funciones, la confidencialidad de los datos personales incluidos en el archivo. Esta obligación se extiende con carácter vitalicio a los miembros de la autoridad de control[297].

La ley portuguesa 67/98 concede una serie de derechos al titular de los datos personales, cuando tal información fuere tratada en forma automatizada: derecho de información (art. 10º); derecho de acceso (art. 11º); derecho de oposición al tratamiento de sus datos personales (art. 12º), etc. A su vez, esta ley (en su mismo articulado) establece sanciones administrativas y penas de multa o prisión de uno a dos años, más sanciones accesorias de acuerdo a la violación sobre ella cometida[298].

La autoridad de control en Portugal es la Comisión Nacional de Protección de Datos (CNPD)[299], cuya función es controlar la aplicación de la ley de protección de datos personales y el respeto por las garantías declaradas en el art. 35 de la

[294] Artículo 5º de la ley 67/98
[295] Artículo 5º de la ley 67/98.
[296] Artículo 14º de la ley 67/98.
[297] Artículo 17º inc. 1º y 2º de la ley 67/98.
[298] Sección IIIª de la ley referida a los delitos (artículos 43 a 49) de la ley 67/98.
[299] Comisión Nacional de Protección de Datos (CNPD – Portugal). Fci.: http://www.cnpd.pt/ (último ingreso el 17/12/2011).

Constitución[300]. Esta comisión se compone[301] de siete miembros de integridad y mérito reconocido, de los cuales el presidente y dos de los vocales son elegidos por la Asamblea de la República. El resto de los vocales se integra con dos magistrados que cuenten con más de diez años de antigüedad y dos personas particularmente competentes designadas por el Gobierno. El artículo 25º de la ley 67/98 establece que los integrantes de la Comisión duran cinco años en el cargo.

El artículo 21º de la ley 67/98 establece que la Comisión Nacional de Protección de Datos es una entidad administrativa independiente con poderes de autoridad, que funciona junto a la Asamblea de la República. Sus decisiones son obligatorias, pero pueden ser objeto de recurso ante el Tribunal Administrativo Superior. Al igual que la autoridad de control española, debe elevar un informe anual a la Asamblea de la República, en el cual detalle la actividad realizada durante el año.

Recientemente, en diciembre de 2011, la CNPD ha aprobado por unanimidad el Dictamen 70/2011 sobre el proyecto de ley propuesto en el uso de video vigilancia en público, teniendo en cuenta que el proyecto de ley adolece de un vicio material de inconstitucionalidad. En su opinión, esta ley disminuye las garantías constitucionales contra el trato abusivo de transferencia de datos personales al Gobierno. En la CIPD se considera que en un Estado democrático de derecho, la norma no puede ser una constante vigilancia de los ciudadanos.

14.- Reino Unido

La historia del derecho a la intimidad, o *privacy*, tiene una gran influencia de la legislación anglo-americana[302]. Mario Losano estudia este proceso y lo divide en cuatro períodos principales a los cuales agregamos un quinto surgido con

[300] Véase el Capítulo IV. Sección I sobre Naturaleza, Atribuciones y Competencias de la Comisión Nacional de Protección de Datos (artículos 21º a 24º) de la ley 67/98.
[301] Véase el Capítulo IV Sección II de la ley 67/98, sobre Composición y Funcionamiento de la Comisión de Protección de Datos (artículos 25º y 26º de la ley).
[302] Centro de Estudios Constitucionales. Cuadernos de Debates Nº 21. Madrid; año 1989. Dentro de esta obra: Losano, Mario G.; "Los orígenes del *Data Protection Act* inglesa de 1984"; p.13.

posterioridad a la sanción y promulgación de la ley británica de protección de datos de 1984:

a) Un primer período se inicia con los orígenes del *Common Law* hasta el ensayo de Samuel Warren y Louis Brandeis, "*The Right to Privacy*", publicado en 1890 en la revista de la Universidad de Harvard (EEUU), con el cual comienza la historia moderna del derecho a la intimidad;

b) Un segundo período, también desarrollado en EEUU, donde se produce el debate sobre el derecho a la intimidad (*privacy*) aplicado a los conflictos relacionados con la prensa. Esta evolución se considera concluida con el escrito publicado en 1960 por William Prosser, en el cual clasifica cuatro violaciones de la *privacy* en una sociedad moderna.

c) Durante el tercer período se produce el traslado del debate sobre la *privacy*, desde EEUU a Gran Bretaña. Se inicia así, en 1961, cuando Lord Mancroft presenta el primer proyecto de ley para la creación de un derecho autónomo a la *privacy*. Es en estos tiempos cuando las tecnologías de la información en general, parecen amenazar la intimidad de las personas y en especial los medios masivos de comunicación social (*mass media*) a través de la radio, la televisión y la clásica prensa escrita. Se debate sobre el derecho de la prensa, la radio y la televisión a introducirse en la vida privada de las personas y a divulgar noticias reservadas. A partir del proyecto de *Lord* Mancroft se realizan otros donde se especifica el concepto de derecho a la intimidad o *privacy*.

d) El cuarto período se inicia en 1969 con el proyecto de Ley Walden (1969) y el proyecto de Ley Baker (1969), que producen un gran cambio en el tema. Estos proyectos de ley no hablan solo del derecho a la intimidad o *privacy* en general, sino que, por primera vez, toman también en consideración la tutela de los datos personales almacenados en sistemas informáticos. Gran Bretaña inicia con estos proyectos el debate de una norma

específica sobre protección de datos personales almacenados en computadoras o sistemas informáticos que configuran la discusión de la *privacy* en el sentido posmoderno. La cuarta fase concluye con la sanción y promulgación de la *Data Protection Act* en 1984.

e) El quinto período se inicia con la sanción y promulgación de la *Data Protection Act* en 1984, y continúa con la sanción, promulgación y posterior aplicación de la nueva Ley de Protección de Datos (*Data Protection Act*) de 1998 y la Ley de Libertad de Información (*Freedom of Information*) del año 2000.

La primera ley de protección de datos personales británica, *la Data Protection Act*, surge el 12 de julio de 1984 luego de un profundo debate en el cual primero es publicado el Libro Blanco sobre Informática e Intimidad (*Computers and Privacy*) en 1975[303] y luego el informe Lindop (*Lindop Report*) en 1978[304].

La Ley de Protección de Datos (*Data Protection Act*) de 1984 fue una norma diferente a las restantes leyes de protección de datos personales vigentes en esos tiempos. Sus principios y reglas se caracterizaron por la generalidad y la flexibilidad, motivos por los cuales pudo ir adaptándose a la dinámica y a las necesidades del cambio tecnológico acontecido en las últimas décadas[305]. Esta ley entró en vigor en forma progresiva, ya que el 12 de septiembre de 1984 comenzó a regir una parte y en una segunda etapa tomó vigencia la otra parte, el 11 de noviembre de 1987, hasta la sanción y promulgación de la Ley de Protección de Datos de 1998.

Al igual que su antecesora, la Ley de Protección de Datos de 1998 se aplica tanto al sector público como al sector privado y exige la inscripción de los archivos en la Oficina del Comisionado para la Protección de Datos.

---

[303] *White Paper: Computers and Privacy*. Editorial HMSO, Londres (GB), 1975.
[304] Cuadernos de Debates Nº 21. Centro de Estudios Constitucionales Madrid; 1989. Dentro de esta obra: Losano, M. *Los orígenes de la Data Protection Act inglesa de 1984*; p.43.
[305] Davara Rodríguez, M. (1998). Op. cit., p. 140.

La Ley de Protección de Datos de 1998 también continuó promoviendo los "*codes of practice*", códigos deontológicos-o de buena práctica profesional-, que fueron incorporados por la ley de 1984. Estos instrumentos permitieron una autorregulación dinámica, de fácil adaptación a los principios de la protección de datos personales y a los nuevos desarrollos de la tecnología.

El derecho británico reconoce ocho principios para proteger al ciudadano, los cuales pueden hacer efectivo el derecho a la protección de sus datos personales. Estos principios son los siguientes: a) Principio de lealtad y licitud, tanto al momento de la recolección datos como durante su tratamiento; b) Principio de adecuación en la utilización, difusión y cesión de los datos con los fines declarados; c) Principio de obligación de respeto a la realidad, a la exactitud y a la actualización de los datos almacenados, con los existentes al momento de su recolección, sin que fueran excesivos para los fines declarados; d) Principio de temporalidad, por el cual los datos no pueden mantenerse registrados por más tiempo del necesario para los fines del tratamiento; e) Principio de reconocimiento del derecho al acceso, a la información, a la rectificación y a la cancelación de los datos almacenados, f) Principio de seguridad, conforme al cual el responsable del tratamiento de los datos personales almacenados debe tomar todas las medidas de seguridad necesarias.

La anterior Ley de Protección de Datos de 1984 había creado la oficina del Registrador Para la Protección de Datos (*The Data Protection Registrar*) y el Tribunal de Protección de Datos (*The Data Protection Tribunal*), dos órganos diferentes que tienen la misión de velar por el cumplimiento de la ley y la protección de los datos personales. Estos órganos de control cambiaron sus nombres con La ley de Protección de Datos de 1998, y la oficina originalmente establecida por la sección 3 (1) (a) de la Ley de Protección de Datos de 1984, como la oficina del Registro de Protección de Datos, mantuvo funciones similares pero cambió su nombre por Oficina del Comisionado de Protección de Datos, (ICO por su sigla en

inglés)[306]. Y el Tribunal de la Protección de Datos modificó su nombre por la denominación de Tribunal de la Información con la Ley de Libertad de Información (*Freedom of Information*) del año 2000.

La Ley de Protección de Datos de 1998 entró en vigencia en el Reino Unido de Gran Bretaña el 1 de marzo de 2000, revocando la Ley de Protección de Datos de 1984. Sus provisiones no tratan de garantizar la privacidad personal a toda costa, sino que buscan encontrar un equilibrio entre los derechos de las personas físicas y los intereses, a veces conflictivos, de quienes tienen razones legítimas para usar la información personal. Es aplicable a algunos registros en papel, así como a los registros informáticos. Es derivada de la Directiva de la UE 95/46/CE que requiere que "los Estados Miembros protejan los derechos fundamentales y las libertades de las personas físicas, en particular su derecho a la intimidad con respecto al procesamiento de los datos personales"[307].

El Comisionado para la Protección de los Datos es nombrado por la Reina de Inglaterra por un período de cinco años, al cabo de los cuales puede ser re-elegido y cuenta con la facultad de nombrar a su suplente y a un equipo de personas que le ayuden en el cumplimiento de sus misiones, siempre dentro del presupuesto que se le asigna. Tiene la independencia necesaria para poder ejercer sus funciones y mantener el registro de archivos con el carácter de publicidad que permita su consulta en forma gratuita. Su misión es velar por el respeto a la ley, en su difusión y conocimiento, orientando y atendiendo las peticiones de asesoramiento e información sobre la creación de códigos de buena conducta, atendiendo las quejas de los ciudadanos sobre el tratamiento de sus datos de carácter personal y teniendo la potestad de inspeccionar, controlar los locales y equipos en los que se tratan o mantienen archivos de datos personales. También se le otorgan las funciones de creación, mantenimiento y actualización del registro de archivos automatizados de datos personales, así como atender a las personas que consideren que sus derechos

[306] Oficina del Comisionado para la Protección de Datos (Reino Unido de Gran Bretaña), fci.: http://www.ico.gov.uk/ (último ingreso el 17/12/2011).
[307] Ibidem.

han sido violentados en el tratamiento de datos de carácter personal. La ley establece que el Comisionado para la Protección de Datos debe mantener un registro público de las personas o sociedades responsables del tratamiento automatizado, donde se registran todas las características de los datos a recolectar y del procesamiento que se fuera a hacer sobre ellos. El registro es público y permite su consulta en la oficina del Comisionado para la Protección de Datos y en las principales bibliotecas del Reino Unido, donde también se encuentra una copia de consulta.

La Oficina del Comisionado para la Protección de Datos puede negar la inscripción de un archivo, pero debe hacerlo en forma fundada y en un plazo de seis meses desde el momento de la solicitud. En estos casos, debe informar al solicitante sobre su derecho de apelación contra la negativa de registración, ante el Tribunal de la Información.

Al igual que otros órganos de control de Europa, el Comisionado también debe enviar un informe anual al Parlamento británico sobre su actividad y gestión.

El Tribunal de la Información fue creado por la Ley de Protección de Datos de 1984 con el nombre de Tribunal de Protección de Datos, que luego fue cambiado por la Ley de Libertad de la Información en el año 2000. Su función es atender los recursos de apelación contra las resoluciones tomadas por el Comisionado para la Protección de Datos y pronunciarse sobre las cuestiones de derecho. Las resoluciones del Tribunal también son apelables ante la jurisdicción ordinaria, pero solamente con relación a la observancia de las normas y su interpretación, ya que la fijación, análisis y pruebas de los hechos eran las fijadas por el propio tribunal.

El Tribunal de la Información se integra por juristas nombrados por el Ministerio de Justicia y las organizaciones representantes de los usuarios. Estos jueces son presididos por un Presidente designado por el Primer Ministro con acuerdo del Ministro de Justicia.

Al igual que en los EEUU, en Gran Bretaña, los archivos de datos sobre solvencia patrimonial y crédito de las personas, conocidos como agencias de referencia de crédito (*Credit reference agencies*), son instituciones que tienen una gran importancia en el trámite de concesión de créditos.

Estas agencias facilitan la información a los interesados en otorgar un crédito, y a su vez reciben de ellos información sobre los solicitantes de crédito. Se produce un intercambio de datos entre las agencias de solvencia patrimonial y las instituciones que tienen contacto directo con los consumidores (*contributing user*) y necesitan tomar decisiones sobre concesión o rechazo de crédito.

Las agencias de información sobre solvencia patrimonial y crédito también facilitan información en forma limitada a otras entidades de las que no reciben información alguna (*non-contributing user*), tales como agentes de bolsa o la Policía.

Dentro de la legislación británica de protección de datos personales, no existe una regulación especial para los archivos sobre solvencia patrimonial o cumplimiento e incumplimiento de obligaciones dinerarias. No obstante, los principios de protección de datos personales consagrados por la ley son relevantes a este tema y tienen permanente aplicación.

Con motivo de la implementación de la Directiva de la UE sobre la privacidad y las comunicaciones electrónicas[308], actualizada para incluir nuevas reglas sobre el uso de las últimas tecnologías y marketing no solicitado, Gran Bretaña dictó en el año 2003 regulaciones sobre la privacidad y las comunicaciones electrónicas. Estas regulaciones son aplicables al envío de mensajes de marketing no solicitados por medios electrónicos como teléfono, fax, correo electrónico y mensajes de texto (SMS).El material de marketing no solicitado transmitido mediante llamadas telefónicas automatizadas para marketing directo debe contar

[308] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de Europa de 12 de julio de 2002 (Unión Europea), relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas. Esta directiva europea, entre otros temas incluye reglas para abordar los mensajes electrónicos no solicitados (correo basura o "spam").

con el previo consentimiento del suscriptor, y debe incluir la identidad de quien llama.

Los suscriptores de llamadas telefónicas de marketing directo no automatizado deben tener la opción de darse de baja. Quienes figuren en el registro del Servicio de Preferencia Telefónica (TPS, por sus siglas inglesas) no deberían recibir ninguna llamada de este tipo a menos que den su expreso permiso.

Las empresas pueden registrarse con TPS para evitar recibir llamadas de marketing no solicitadas. Los suscriptores individuales y corporativos pueden registrar su objeción a recibir faxes de marketing directo no solicitados inscribiendo su número en el Servicio de Preferencia de Fax (FPS, por sus siglas inglesas).

El material de marketing no solicitado por correo electrónico (incluye mensajes en texto y gráficos y mensajes electrónicos) debería enviarse exclusivamente si la persona física "se ha dado de alta" para recibirlos, salvo en el caso de que la dirección electrónica de la misma haya sido obtenida en el contexto de una relación comercial. A la persona física se le debería dar siempre la oportunidad de darse de baja y, de ese modo, dejar de recibir mensajes electrónicos.

La Oficina del Comisionado para la Protección de Datos de Gran Bretaña (ICO) está trabajando en colaboración con sus homólogos europeos y de EEUU para intentar reducir el correo basura. Estas regulaciones son aplicables sólo a correo basura enviado desde dentro de la UE. Actualmente no existe ninguna legislación que cubra el correo basura que se envía a direcciones comerciales.

15.- Suecia

Suecia dictó su primera legislación sobre la protección de datos por medio de su Ley de Datos (*The Data Act*) número 1973/289 vigente a partir del 1 de julio de 1973[309], siendo modificada, primero en 1989 y luego remplazada en 1998 por la ley

[309] Davara Rodríguez, M. (1998). Op. cit., p.173.

de Protección de Datos (*The Personal Data Act*) Nº 1998/204, que comenzó a regir plenamente a partir del 30 de septiembre de 2001[310].

El marco legislativo en materia de datos personales se completa en Suecia con la Ley de Información de Crédito (*The Credit Information Act*) promulgada en 1973 y la Ley de Recuperación de Deudas (*The Debit Recovery Act*) promulgada en 1974.

La vigente ley de Protección de Datos 1998:204 sigue el lineamiento de la Directiva 95/46/CE y contiene los principios clásicos de la protección de datos tales como el de finalidad y adecuación al fin, de seguridad, del secreto profesional, de duración, de conservación limitada y de exactitud y actualización. En ella también se exige al titular del banco de datos, confidencialidad y de seguridad en el tratamiento. Textualmente expresa que el propósito de su existencia el proteger a las personas contra la violación de su integridad personal mediante el procesamiento de sus datos personales[311].

Al igual que el resto de la legislación europea, contiene una sección de definiciones y conceptos, establecidos al efecto de su interpretación y aplicación. Entre ellos se destaca el concepto de datos personales, sobre los que textualmente entiende que son "toda clase de información que directa o indirectamente pueda ser referida a una persona natural que está viva"[312].

La ley de protección de datos alcanza a todos los procesamientos de datos personales que sean completa o parcialmente automatizado, alcanzando también a otros procesamientos de datos personales, cuando estos datos sean incluidos o dirigidos a formar parte de una colección organizada y estructurada de datos

[310] Aun cuando la Ley de Datos Personales suecaNº 1998/204 entró en vigencia el 24 de octubre de 1998, siguió regiendo para aquellos procesamientos de datos personales realizados antes de esa fecha, la Ley de Datos de 1973 (*The Swedish Data Act* de 1973), siendo aplicable la Ley de Protección de Datos de 1998 (*The Personal Data* Act Nº 1998:204) para todos los procesamientos de datos, independientemente de la fecha en que fueron realizados, a partir del 30 de septiembre de 2001.
[311] Ley de Datos Personales Nº 1998:204, Provisiones Generales, Primera Sección.
[312] Ley de Datos Personales Nº 1998:204, Tercera Sección.

personales, que esté dispuesta para la investigación o compilación de acuerdo con un criterio específico[313]. En cambio, su ámbito de aplicación no alcanza al procesamiento de datos personales que una persona natural realiza en el curso de actividades de una naturaleza puramente privada[314].

La ley sueca de protección de datos personales se aplica a todos los bancos o bases de datos personales, sean de titularidad pública como privada que se encuentren en el territorio de Suecia, y extiende su ámbito de aplicación también a los bancos de datos personales establecidos en un tercer país, que procese datos personales por medio de equipos situados en Suecia[315].

A los efectos de un mejor control, el responsable del banco o base de datos tiene la obligación de notificar por escrito a la Autoridad de Control, antes de iniciar un procesamiento de datos personales[316], y en la sección novena de la ley, se obliga al responsable del banco o base de datos, a procesar solamente datos personales en forma lícita, correcta y de acuerdo con los principios de la buena fe. Solo autoriza a recoger datos para propósitos específicos y justificados, enunciados en forma explícita. Los datos recogidos deben ser correctos, actualizados, adecuados y relevantes en relación con el propósito del procesamiento[317].

La autoridad de control sueca es la *Datainspektionen* (Junta de Inspección de Datos)[318], autoridad pública que actúa a través de un equipo de empleados públicos, que en su mayoría son abogados, bajo la dirección de un Director. La función de este organismo público es proteger la intimidad de las personas en la sociedad de la información sin exigir prevenciones innecesarias que compliquen el uso de las nuevas tecnologías.

---

[313] Ley de Datos Personales Nº 1998:204, Quinta Sección.
[314] Ley de Datos Personales Nº 1998:204, Sección sexta.
[315] Ley de Datos Personales Nº 1998:204, Cuarta Sección.
[316] Ley de Datos Personales Nº 1998:204, Sección treinta y seis.
[317] Ley de Datos Personales Nº 1998:204, Sección novena.
[318] Junta de Inspección de Datos, (autoridad de control en materia de protección de datos de Suecia). Fci.: http://www.datainspektionen.se (último ingreso el 17/12/2011).

La Junta de Inspección de Datos tiene facultades para autorizar la creación de archivos y dictar instrucciones detallando su contenido, los límites del tratamiento y la forma de recolección de los datos. Ejerce sus funciones y controles por iniciativa propia o a instancia de parte. Sus decisiones pueden ser apeladas.

Los artículos 20 a 24 de la ley 1998/204 contemplan sanciones a quienes infrinjan la ley o las instrucciones de la Junta de Inspección de Datos. Las sanciones pueden llegar a la pena de prisión, y a la confiscación de archivos. En el caso de que se hubiera causado un daño al titular de los datos por informaciones inexactas, el responsable del archivo puede ser sancionado con multas y debe responder por el daño causado ante el titular de los datos.

La Junta de Inspección de Datos puede conceder autorizaciones para la creación de registros de personas y su explotación a petición del titular del archivo y en ese caso dictará instrucciones sobre la información personal que pudiera ser incluida en el registro de personas, sobre la ejecución del proceso automático de datos, sobre el equipamiento técnico, sobre la comunicación a las personas interesadas, sobre la información personal que debe ser objeto de acceso y sobre control y seguridad.

La Junta de Inspección de Datos tiene la obligación de velar para que no se produzca ninguna acción contraria a la ley y para que no exista intromisión en la vida personal del titular del dato. A tales efectos ejerce la función inspectora y está autorizada a ingresar en los locales en los que se lleve a cabo el tratamiento automatizado de datos, con pleno acceso a los documentos que conciernan al tratamiento de datos personales.

La ley exige un registro de personas y direcciones que será llevado en forma automatizada y que se utilizará para actualizar, completar y controlar la información de otros registros de personas y, por medio de una recuperación selectiva, seleccionar información personal. Este registro podrá ser consultado tanto por los particulares como por las autoridades.

En Suecia la regulación de los archivos de datos personales de información sobre riesgo de crédito no está regulada por la Ley de Protección de Datos, sino por la ley 1973/1173, que regula la recolección y el tratamiento de datos personales de crédito. La ley permite que, en determinados supuestos, los datos personales de crédito sean procesados sin el consentimiento del afectado. La ley también protege al afectado, ya que contiene ciertas restricciones con respecto a los datos personales que pueden recabarse y tratarse sin su consentimiento. No pueden incluirse datos sensibles, ni datos sobre deudas o incumplimientos de obligaciones dinerarias que no hayan sido reconocidos por tribunales o conocidos por motivos de quiebra, suspensión de pagos o bancarrota del afectado.

El art. 3 de la ley sueca obliga a las empresas que prestan servicios de información sobre solvencia patrimonial y crédito, a solicitar un permiso a la autoridad de control antes de comenzar sus actividades. Tal permiso sólo podrá obtenerse cuando sea necesario llevar a cabo este tipo de actividades por razones de interés público y cuando el titular del banco de datos asuma el compromiso de contratar un experto para que dirija las actividades. El otorgamiento del permiso será por un tiempo de 10 años como máximo, después de los cuales deberá solicitarse de nuevo si se desea continuar con las actividades de prestación de servicio de información sobre solvencia patrimonial y crédito. El permiso puede ir acompañado de ciertas líneas directrices que habrán de ser tenidas en cuenta por la empresa a la que se concede.

La empresa está obligada a notificar a la autoridad ante cualquier cambio en las circunstancias que se tuvieron en cuenta para conceder el permiso.

La ley contiene preceptos para proteger al afectado; así, el art. 5 expresa que no podrá utilizarse la información de forma tal que pueda dar lugar a conclusiones incorrectas y malentendidos. Además, el art. 8 añade que no podrán mantenerse en el archivo los datos que tengan una antigüedad mayor de tres años.

Los arts. 19 a 23 imponen penas a las personas que lleven a cabo las actividades que regula esta ley de forma negligente o incumplan los preceptos de la misma.

El art. 140 concede al afectado el derecho de acceder a sus propios datos, y el art. 12 impone al responsable del banco de datos la obligación de hacer las investigaciones necesarias para comprobar la veracidad de los datos registrados cuando tenga razones para pensar que los datos no son del todo correctos. Y, en el caso de que se pruebe que dichos datos no son correctos, deberá destruirlos inmediatamente e informar a las personas que los hayan recibido durante los últimos doce meses.

16.- Noruega

En el Reino de Noruega[319] la protección de datos personales se encuentra regulada por la Ley sobre el Tratamiento de Datos Personales Nº2000-04-14-31[320]. Esta norma fue promulgada en el año 2000, entró en vigor el 1° de enero de 2001 y sufrió diferentes modificaciones, pero la más reciente data de junio del año 2009.

En su contenido podemos encontrar que el capítulo I se ocupa del objeto y del ámbito de aplicación de la ley. Cuestiones tales como los propósitos de la ley, las definiciones, los alcances, la competencia geográfica, la relación con otras leyes y con el derecho de acceso legal, junto con la relación con la libertad de expresión son los temas que se desarrollan en este capítulo.

[319] El Reino de Noruega optó por permanecer fuera de la Unión Europea durante un referéndum en 1972 y nuevamente en 1994. Sin embargo, Noruega, junto con Islandia y Liechtenstein, participan en el mercado único de la UE a través del acuerdo del Área Económica Europea. Las principales razones por las que la población noruega rechaza entrar en la UE son el gran nivel de vida del que gozan debido a los grandes ingresos por producción del petróleo; el país escandinavo en la UE tendría, entonces, un papel de donación de recursos económicos a los países más débiles.

[320] Texto de la Ley en castellano. Fci: http://translate.googleusercontent.com/translate_c?hl=es&prev=/search%3Fq%3Dhttp://www.datatilsynet.no/%26hl%3Des%26rlz%3D1G1TSLA_ESAR439%26prmd%3Divns&rurl=translate.google.com.ar&sl=no&u=http://www.lovdata.no/all/nl-20000414-031.html&usg=ALkJrhjyJa6OcSG3JXJwaBLo7NHXoOLQ-Q (último ingreso el 7 de agosto de 2011).

El capítulo II establece las reglas generales y requisitos básicos para el manejo o tratamiento de datos personales, condiciones para el procesamiento de datos personales en general y de datos personales sensibles en particular, para el registro de antecedentes penales, para el ejercicio del derecho a la identidad personal, etc.

El capítulo III establece la información que se debe brindar al afectado sobre el tratamiento de datos personales, tales como el derecho de acceso, la divulgación de información cuando los datos son recogidos de la registrada, la divulgación de información cuando los datos se recogen de una persona distinta del registro, el deber de la utilización de perfiles personales, el derecho a la información acerca de las decisiones automatizadas, las excepciones al derecho a la información, la forma en que la información será proporcionada.

El capítulo IV se refiere a otros derechos de los registrados, tales como el derecho a exigir el procesamiento manual, la rectificación de la información personal deficiente y la prohibición en contra de almacenamiento de información personal innecesaria.

El capítulo V de la ley sueca se refiere a la transferencia de datos personales en el extranjero, las condiciones básicas y las excepciones. El capítulo VI se ocupa de la notificación y requerimiento de licencia y concesión de servicio, de la decisión de conceder una licencia y de los términos en que se la concede.

El capítulo VII se ocupa de la vigilancia de televisión. Establece una definición y un reglamento, determina el alcance y los requisitos básicos para su monitoreo, la divulgación de las grabaciones de imágenes tomadas por video vigilancia.

El capítulo VIII define el control y sanciones. Se ocupa de la organización de los datos y las tareas de control que lleva adelante la Junta de Protección de Datos, la confidencialidad, las sanciones por violación a la ley.

La autoridad de control es la Junta de Protección de Datos de Noruega[321]. Tiene la tarea de ayudar a proteger la intimidad de las personas violada por el tratamiento de datos personales. Los datos personales serán tratados de acuerdo con las consideraciones básicas de política, tales como la necesidad de protección de la integridad personal y la privacidad. El procesamiento de datos es principalmente regulado por la Ley sobre el tratamiento de datos personales de 14 de abril de 2000 (Ley de datos personales) y la Ley de registros de salud y el procesamiento de información de salud (Ley del Sistema), de 18 mayo de 2001.

La Inspección es un organismo independiente, aun cuando administrativamente depende del Ministerio de Administración Gubernamental y Asuntos de la Iglesia. La independencia mencionada significa que el Ministerio no puede dar instrucciones a La Inspección; o expresado de otra forma, que el Ministerio no puede ejercer la Inspección de Datos de la autoridad bajo la Ley de Datos de Carácter Personal y Sistemas de Archivos. Las decisiones de la Inspección de Datos pueden ser apeladas ante la Junta de Apelaciones. El Comité presenta su propio informe anual.

Para identificar los riesgos a la vida privada y dar consejos sobre cómo pueden ser evitados o limitados, la Junta de Inspección de Datos Personales debe dar información de los acontecimientos nacionales e internacionales en el tratamiento de datos personales, y los problemas asociados con este tratamiento. La participación en consejos y comités es una parte importante del trabajo de Protección de Datos. También como un órgano consultivo dictamina sobre asuntos que pueden tener consecuencias relacionadas con la privacidad.

La Junta de Inspección de Datos lleva un registro público de todo el procesamiento de los datos personales. Realiza la supervisión activa y los controles de procedimiento que determinan las leyes y reglamentos para el tratamiento de datos personales.

[321] Junta de Protección de Datos de Noruega: http://www.datatilsynet.no/ (último ingreso el 17/12/2011).

La Inspección también motiva y apoya a las empresas que voluntariamente han nombrado a su defensor del pueblo de privacidad. Otro papel importante de la Inspección es su rol mediador; en este sentido, realiza asesoramiento y brinda información a las personas. Para crear conciencia e interés sobre los temas de privacidad relacionados, la Inspección participa activamente en el debate público sobre el tema y hace hincapié en la práctica de la apertura pública, informa en su sitio web sobre todas las novedades y documentos necesarios para la actualización de la información.

CAPÍTULO III: PROTECCIÓN DE DATOS EN AMÉRICA

Ya explicamos en el capítulo I que el derecho a la intimidad es el derecho núcleo desde el cual se desarrolla el derecho a la intimidad, aun cuando en su evolución se independiza, se hace autónomo y crece como un derecho nuevo, distinto, que ya no sólo protege los datos íntimos de una persona sino también aquellos que sin ser íntimos se refieren a ella.

Con esta idea podemos iniciar este capítulo III sobre la protección de los datos personales en América, diciendo que la protección del derecho a la intimidad en este continente fue incorporada en noviembre de 1969 por la Convención Americana sobre Derechos Humanos[322], también conocida como Pacto de San José de Costa Rica[323], en la cual encontramos diferentes normas que dan fundamento a los derechos relacionados con el derecho a la protección de los datos personales. Así, el artículo 1º[324] compromete a los Estados firmantes a legislar contra la discriminación por motivos de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier índole. Otros artículos[325] contienen declaraciones que protegen la honra y la dignidad de las personas; así, el art. 11 enuncia en su inciso 1º, que "*Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación*".

[322] La Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica), puede ser consultada en el sitio web http://www.cajpe.org.pe/RIJ/bases/instru/ib1. HTM.
[323] Fue ratificada en la República Argentina por medio de la ley 23.054.
[324] El artículo 1º del Pacto de San José de Costa Rica, textualmente expresa que "Los Estados Partes en esta Convención se comprometen a respetar los derechos y libertades reconocidos en ella y a garantizar su libre y pleno ejercicio a toda persona que esté sujeta a su jurisdicción, sin discriminación alguna por motivos de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social".
[325] Existen diferentes artículos del Pacto de San José de Costa Rica, relacionados directa o indirectamente con la protección de los datos personales, entre ellos, y a modo de ejemplo, podemos mencionar el art. 12 sobre la libertad de conciencia y religión; el artículo 13º sobre la prohibición de realizar apología al odio racial, nacional o religioso; artículo 16 sobre la libertad de asociación con fines religiosos, ideológicos o políticos; etc.

Luego llegará la incorporación del instituto del *habeas data* en la Constitución de la República Federativa de Brasil en 1988, con la cual se inicia en América un proceso de reformas constitucionales que incluirán una garantía constitucional[326] específica para controlar los bancos de datos públicos y privados, a los efectos de proteger los datos de carácter personal y permitir la toma de conocimiento de la información personal almacenada en bases, archivos o bancos de datos públicos y privados.

EEUU y Canadá dictaron las primeras normas sectoriales de protección de datos personales en el continente americano en el siglo pasado. El resto de las naciones de América, todas más retrasadas en el uso de la tecnología que los países del norte, recién comenzaron a legislar sobre este tema en el presente siglo. Seguramente el menor uso de la tecnología informática fue un factor determinante por el cual las normas sobre protección de datos personales demoraron su llegada en el centro y en el sur de América, e incluso en algunos Estados todavía están en proyectos de legislación o bien deben ser mejoradas.

Las primeras leyes latinoamericanas sobre protección de datos personales surgieron en Chile (1999) y en Argentina (2000). Varios años más tarde lo hicieron

[326] Víctor Ortecho Villena entiende que las garantías constitucionales son las seguridades o protecciones que dispone la Constitución a favor de los derechos y libertades fundamentales y demás derechos constitucionales. Estas medidas de protección, más que derechos son medios de defensa que el ordenamiento constitucional asigna a los organismos jurisdiccionales, y que consisten en mecanismos procesales que deben emplearse para contener los excesos del poder, que generalmente vienen de autoridades y funcionarios del Poder Ejecutivo. Las libertades como acciones políticas de eximición o liberaciones a acciones de oposición, no tendrían mucha fuerza o resultarían anárquicas si no hubiera derechos que reconozcan su ejercicio: y ambos resultarían líricos si es que no hubiera resortes jurídicos que les den seguridad de ser practicados, esos resortes son las garantías. Si tratamos de diferenciar resumidamente los términos libertad, derecho y garantía, tendríamos que decir que la libertad como acción liberadora es la esencia del derecho. El derecho es la facultad jurídica y legal del ejercicio de la libertad, y la garantía es el amparo para la cristalización de la libertad y del derecho. La libertad es el contenido y la esencia, el derecho es la forma del contenido, y la garantía es el ropaje y continente de los dos anteriores. Bidart Campos entiende que las garantías son las instituciones de seguridad creadas a favor de las personas, con el objeto de que dispongan del medio para hacer efectivo el reconocimiento de un derecho. Son remedios jurisdiccionales que dan origen a una pretensión que solo puede dirigirse al poder público porque es demanda de tutela para que ampare, asegure, restaure o haga efectiva una pretensión jurídica, en la que puede existir un derecho.
Ortecho Villena, V. *Jurisdicción y Procesos Constitucionales*. 7ª ed. Editorial Rodhas. Lima (Perú), 2002, p. 93.

Perú y México. Actualmente Brasil y otros países discuten sus proyectos legislativos. Sin embargo, en todos los casos nos encontramos ante leyes o proyectos de leyes que diseñan organismos de control dependientes del Poder Ejecutivo del Estado, e ineficaces para la protección de los datos de carácter personal. Quizás, el principal problema del diseño de las agencias o autoridades de control para la protección de datos en Sud-América y Centro América, sea, por ejemplo, la falta de presupuesto o las sistemáticas crisis económicas que impiden a los gobiernos de la región dar la importancia que este tema se merece, ante otras urgencias humanas básicas todavía irresueltas.

A continuación estudiaremos el derecho a la protección de datos de los diferentes Estados del continente americano. Por los motivos antes explicados, partiremos del derecho a la intimidad para encontrar al derecho a la protección de los datos personales.

1.- Estados Unidos de América.

La doctrina jurídica, las normas y la jurisprudencia de los EEUU de América son antecedentes fundadores en materia de protección de datos personales. Los juristas norteamericanos Samuel Warren y Louis Brandeis construyeron el moderno concepto jurídico de derecho a la vida privada (*privacy law*), al publicar un embrionario escrito en la revista de la Universidad de Harvard titulado *The Right to Privacy*[327].

Cierto es que a Warren y a Brandeis los guiaba el interés por proteger un derecho de clase; buscaban evitar la intromisión de la prensa en la intimidad de una clase social alta, acostumbrada a un estilo de vida con habituales reuniones, fiestas y acontecimientos sociales. Ellos nunca imaginaron que sus esfuerzos intelectuales en la redacción del precursor ensayo *The Right to Privacy,* terminarían creando el primer antecedente doctrinario para la formación del nuevo derecho a la auto-

[327] Warren, S.; Brandeis, L. "The Right to Privacy". Revista de la Universidad de Harvard: 4 Harv. L. Rev. Cambridge, Massachusetts (EEUU), 1890, p. 193.

determinación informativa. Nunca pensaron que estaban prestando sus servicios intelectuales para la creación del antecedente doctrinario fundante del nuevo derecho humano de tercera generación relativo a la protección de los datos personales.

Samuel Warren, Senador de los EEUU, consideró que la prensa de Boston lo había afectado al divulgar información sobre el matrimonio de su hija. Quizás por este motivo, junto al jurista Louis Brandeis (luego miembro del Tribunal Supremo de Justicia de los EEUU), estudiaron los precedentes jurisprudenciales, en busca de una norma que permitiera proteger la intimidad de las personas. Documentaron antecedentes judiciales del *Common Law*[328] sobre un derecho general a la *privacy*, desarrollado a través de los casos de violación de la propiedad, de la confianza, del derecho de autor y en casos de difamación. La investigación llegó a la conclusión de que el derecho general a la vida privada (*right to privacy)*, era idóneo para dar protección jurídica a los casos de violación de la privacidad por medio de la prensa.

La doctrina del derecho a la vida privada (*Privacy Law*), aportó una nueva interpretación de los precedentes judiciales del derecho de los EEUU, ya que antes de esta doctrina, se entendía que el *Common Law* solo protegía personas físicas o bienes materiales a través del derecho de propiedad, de tal modo que la intimidad relativa a la persona recibía una tutela solo indirecta y a menudo incompleta. Lo novedoso del ensayo fue el reconocimiento a una tutela jurídica sobre bienes inmateriales como los pensamientos, las emociones y las sensaciones de una persona física

Durante los cincuenta años siguientes a la publicación del ensayo de Warren y Brandeis se discutieron centenares de casos de violación al derecho a la intimidad personal por difusión de información privada en los medios masivos de

[328] Entiéndase por *Common Law* al sistema judicial anglosajón.

comunicación[329]. El derecho a la vida privada se fue configurando como un derecho autónomo, cuya protección no era aún más que indirecta.

Muchos años más tarde, se dictaron en los EEUU las primeras normas que buscaron proteger la información personal. La *Freedom of Information Act* (Ley de Libertad de la Información, FOIA)[330] como la *Fair Credit Reporting Act* (Ley de Equidad Financiera de 1978)[331] y la *Privacy Act* (Ley de protección de la Intimidad)[332].

El sistema jurídico anglosajón ha preferido promulgar normas sectoriales en materia de protección de datos personales. Se llama así a esta clase de leyes, porque son específicas para determinados sectores o materias. Hoy encontramos en la legislación de los Estados Unidos de América las siguientes normas relativas a la registración y almacenamiento de datos:

a) Ley de Protección de la Intimidad de 1974 (*Privacy Act*): busca proteger la intimidad de las personas cuyos datos personales figuran en bancos de datos del gobierno. Sus principios básicos son los siguientes: prohibición de la existencia de bancos de datos secretos de información personal; posibilidad del individuo de conocer que información existe acerca de él y cuál va a ser su uso; derecho de las personas a corregir o ratificar la información registrada sobre ella; prohibición de uso de la información personal sin el consentimiento de titular de los datos, para otro propósito diferente de aquel para el cual fue recopilado; toda entidad que recopile, use o distribuya información personal debe establecer los medios necesarios para asegurar su fiabilidad y prevenir los posibles abusos que se puedan realizar con la misma. Finalmente, la *Privacy Act*[333] (ley de protección de la

[329] Alderman, E.; Kennedy C. *The Right to Privacy*. Ed. Random House, New York, 1997; p. 154

[330] Freedom of Information Act (Ley de Libertad de la Información - EEUU), FOIA. Fci.: http://www.usdoj.gov/04foia/1974compmatch.htm

[331] Fair Credit Reporting Act (Ley de Equidad Financiera de 1978. Esta ley fue modificada en diferentes momentos. Fci.: http://www.ftc.gov/os/statutes/fcradoc.pdf

[332] Gozaíni, O. (2001). Op. cit. La *Privacy Act* de 1974 con sus modificaciones, puede ser consultada en el CD-Rom anexo a esta obra.

[333] The Privacy Act (Ley de Protección de la Intimidad) de 1974. Fci.: http://www.usdoj.gov/04foia/1974compmatch.htm

intimidad) de 1974[334], que luego sufrió enmiendas surgidas a partir de las leyes de Libertad de Información (*Freedom of Information Act*) y de Procedimientos Administrativos, sustentando el derecho del pueblo a obtener información pública. La *Privacy Act* es una ley más general, que otorga a toda persona física el derecho a proteger su intimidad, frente a la información contenida en los registros del gobierno federal.

La *Privacy Act* exige a las entidades públicas que solo lleven archivos de datos personales que guarden relación con los fines para los cuales han sido creadas. Los bancos de datos personales están obligados a obtener la información directamente del sujeto pertinente, a mantener los datos actualizados y a conceder al individuo el derecho de acceso a los mismos (con limitaciones en el caso de los archivos pertenecientes a los servicios de inteligencia, inmigraciones y aquellos relacionados con la lucha contra el narcotráfico).

Los bancos de datos necesitan contar con el consentimiento libre y expreso del interesado para poder difundir los datos personales allí registrados, salvo cuando su difusión responda a los fines para los cuales se recogió la información, o cuando se trate de información requerida por la justicia, el Congreso, los archivos nacionales, los servicios de estadísticas o aquellos relativos a infracciones de tránsito.

b) Ley de protección de datos del sector de la educación: protege la información registrada en instituciones educativas públicas. Sus principales puntos son: los datos sólo pueden ser recopilados por aquellas personas u organismos autorizados por ley; los estudiantes y sus padres tienen el derecho de acceso a las informaciones educacionales sobre ellos; solamente se permite la comunicación de esta información a las instituciones educativas públicas para el uso administrativo y a las autoridades en los supuestos legales;

[334] Alderman, E.; Kennedy C. (1997). Op. cit., p. 1.

1) Ley de protección de la privacidad financiera *Fair Credit Reporting Act*[335] de 1978: proporciona protección a los individuos, restringiendo el acceso del gobierno a las informaciones sobre los clientes de los bancos e instituciones financieras, estableciendo así un cierto grado de confidencialidad de los datos financieros personales. Esta ley protege al cliente de establecimientos de crédito contra la violación de su privacidad por parte de las agencias de información, sin tener en cuenta el método utilizado para su registro.

2) Ley de libertad de información[336] de 1966 (*Freedom of Information Act)*: establece el derecho de las personas a acceder a los datos sobre ellos almacenados. Consagra el principio según el cual la información contenida en los documentos públicos es de libre acceso al pueblo norteamericano. La ley de Libertad de Información (FOIA), es otra norma relacionada con el derecho a la información, es una forma de *habeas data* que permite el acceso a toda clase de documentación o archivo gubernamental. Su contenido fue enriquecido en el tiempo. Entró en vigencia en 1966, y fue modificada en 1974 como consecuencia del *Watergate*, y durante el gobierno de Ronald Reegan, en 1986.

Con el objeto permitir el acceso de las personas a la información en poder de la administración pública, la "FOIA" obliga a la administración pública a llevar listados actualizados que permitan al público conocer el tipo de información contenida en los registros de cada organismo perteneciente al Estado. El solicitante debe declarar una razón de necesidad y la oficina pública no puede negarse, salvo que expusiera razones debidamente fundadas. Pero cuando el fundamento para denegar el acceso a la información esté basado en la calificación de información confidencial de los datos solicitados, la carga de la prueba corresponde al organismo

[335] *Fair Credit Reporting Act*. Fci.: http://www.ftc.gov/os/statutes/fcradoc.pdf (ultimo ingreso el 26/12/2012)
[336] Freedom of Information Act. Fci.: http://www.usdoj.gov/04foia/1974compmatch.htm

público involucrado. La negativa a exponer la información solicitada, deja abierta al solicitante la vía judicial.

La norma bajo análisis posibilita con ciertas excepciones que toda oficina gubernamental expida información específica referida al contenido de archivos, fichas o informaciones contenidas en un banco de datos determinado y perteneciente a un período de tiempo limitado. El gobierno debe acceder a la petición aunque puede cobrar los costos de búsqueda y reproducción de la información si supera un mínimo. En caso de demora o negativa de la dependencia, se puede accionar legalmente contra ella, y si se demuestra una actuación ilegítima por parte del funcionario que negó la información, puede sufrir sanciones, quedando el Estado obligado a resarcir los daños y perjuicios que pudieran haberse ocasionado.

No impone como requisito una necesidad subjetiva entre el requirente y la información, e incluso obliga a las oficinas gubernamentales a brindar al público datos sobre su organización y sobre la forma para adquirir información sobre su actividad y archivos. Consagra también el principio operativo de la publicidad de los actos de gobierno y el acceso a bancos, archivos, expedientes específicos, etc.

Las oficinas gubernamentales deben fijar un costo razonable que contemple si el interés es comercial, científico, educativo, personal o general.

Los jueces federales pueden exigir la reproducción de archivos y de información denegada, fijando a la oficina en cuestión un plazo no superior a treinta días, además de las posibles sanciones. Toda solicitud de informes deberá ser respondida por la oficina en un plazo de diez días hábiles, aceptando apelaciones de su decisión con respuesta dentro de los 20 días siguientes a su interposición. La complejidad de los archivos y las circunstancias del caso pueden justificar un plazo mayor, dada la razonabilidad de la situación.

La ley establece excepciones que están referidas a la existencia de una orden de defensa nacional o de política internacional que determine la clasificación de

secreto o reserva de la información peticionada. Tal limitación también puede surgir por una disposición expresa del Parlamento, referida a secretos comerciales; documentación privada de terceros, fichas con contenidos personales, informes de salud, información sobre las fuerzas policiales o de seguridad que al develarse pongan en peligro la integridad física de sus integrantes; información financiera bajo secreto bancario.

Las oficinas gubernamentales tienen la obligación anual de elevar un informe al Congreso y al Presidente de la Nación sobre la cantidad de solicitudes, denegaciones, apelaciones administrativas, órdenes judiciales y sanciones aplicadas. Tal exigencia posibilitó el necesario control parlamentario que resulta esencial para el equilibrio de poderes y para evitar que el Congreso se transforme en un mero espectador y continuo solicitante de informes, de los cuales sólo recibirá respuesta si dichos informes no afectan los intereses del Ejecutivo.

Cuando la FOIA se refiere a las oficinas gubernamentales, resultan comprendidas todas las dependencias del departamento ejecutivo entendidas en forma amplia, y las agencias regulatorias independientes.

3) Legislación Estatal. Además de las leyes federales ya mencionadas, cada Estado dicta sus propias leyes. En muchas de estas normas se exige que los datos sean relevantes, actualizados y precisos, además se prohíbe su difusión sin autorización. Falta legislación que regule las prácticas de las instituciones privadas respecto de sus bancos de datos de información personal. Oscar Puccinelli opina que esto sucede porque aún no está claro el significado del concepto de "privacidad de la información"[337]. Al igual que las leyes federales, las estatales exigen que se informe sobre la finalidad del tratamiento de datos personales, en forma análoga al principio de finalidad, recogido por la mayoría de las leyes europeas.

[337] Puccinelli, O. (1999). Op. cit., p. 188.

1.1.- Autoridad de aplicación en EEUU

Los EEUU carecen de un organismo de control en materia de protección de datos personales como los que existen en Europa. Como hemos explicado *ut supra*, el sistema jurídico norteamericano no legisla con leyes de alcance general u ómnibus; por el contrario, ha regulado la materia con diferentes leyes sectoriales. Este es el motivo por el cual el sistema no ha diseñado una magistratura o institución especializada en la vigilancia y control de la aplicación de normas sobre protección de la intimidad, ya que esta función le corresponde a la autoridad de aplicación de cada uno de los sectores sobre los cuales se dictaron leyes sectoriales.

1.2.- Bancos de Datos de Información de Crédito

Los bancos de datos de información personal sobre crédito cumplen, en economía de los EEUU, la función de ayudar a las empresas a evaluar los riesgos de aumentar un crédito, financiar su pago, cobrar deudas vencidas y localizar a determinados individuos.

La ley impone a las agencias de información sobre crédito la obligación de tratar datos personales para un fin específico y limita la posibilidad de transmitir datos sobre personas físicas a terceros, sólo en las siguientes circunstancias: 1) En cumplimiento de una orden judicial. 2) En respuesta a las instrucciones del afectado realizadas por escrito. 3) Cuando sea necesaria para una operación de crédito que determine la extensión del crédito de un individuo o la revisión de una cuenta personal. 4) Por cuestiones de índole laboral. 5) Cuando sea necesaria para la contratación de un seguro. 6) Cuando sea necesaria para la inscripción de la candidatura de un individuo. 7) Cuando sea necesaria para la obtención de una licencia de conducir de un individuo. 8) Para cualquier otro beneficio otorgado por el gobierno, que requiera la consideración de la situación y responsabilidades financieras del individuo. 9) Cuando sea necesaria para concretar una transacción o negocio legítimo del que el individuo afectado forme parte.

Al limitar la cesión o transferencia de datos permisibles, la ley federal obliga implícitamente a las agencias a recoger exclusivamente datos personales sobre crédito para alguno de los fines mencionados. Las leyes estatales sobre crédito contienen restricciones similares a las de la ley federal, con lo que indirectamente imponen igualmente la existencia de un fin específico.

Tanto las leyes federales como las leyes estatales de los Estados Unidos contienen principios similares al principio de finalidad recogido en las leyes de protección de datos europeas. Aun así, el uso de información sobre crédito para actividades de marketing directo prueba que el concepto de fin se interpreta de una forma mucho más amplia en las agencias de información sobre crédito de Estados Unidos que por las mismas agencias en Europa.

Como hemos visto, tanto las leyes federales como las estatales enumeran de forma limitativa los fines por los que la información de crédito puede transmitirse a terceros. La intención es limitar el uso de datos personales sobre créditos para fines secundarios.

Sin embargo, no resulta fácil saber cuándo la ley federal considera que una empresa que obtiene datos personales para un fin legítimo enumerado por la ley está usando los datos para fines secundarios.

La prohibición legal existente en Estados Unidos para usar los datos personales sobre crédito para fines secundarios permite excepcionalmente el uso de estos datos cuando sean necesarios para cualquier negocio legítimo. Este requisito permite un uso bastante amplio de datos personales.

En contraposición a la legislación europea, en los Estados Unidos no existe una prohibición general de la recolección de datos innecesarios. No obstante, las agencias no son propensas a recoger datos innecesarios debido a la configuración del sistema de acuerdo con los fines legales.

Las obligaciones legales derivadas de la legislación de los EEUU responden al principio europeo de limitación de conservación de datos personales, y aunque la ley federal no requiere de forma explícita la destrucción de información sobre crédito obsoleta, las agencias de información sobre crédito no pueden transmitir cierto tipo de datos personales una vez pasados los períodos de tiempo establecidos por la ley. Por ejemplo, datos de quiebras y suspensiones de pago después de diez años, sobre condenas judiciales después de siete, etc. El efecto de estas prohibiciones legales es la imposición indirecta de un límite a la conservación de esos datos particulares.

Las personas también poseen los derechos de acceso y rectificación de datos en los bancos de datos sobre información crediticia, en forma comparable a la legislación europea. La legislación federal, al igual que la estatal, garantiza a los afectados el derecho a obtener acceso a los datos sobre crédito que les conciernan, incluyendo información sobre las fuentes y las personas a las que dichos datos han sido comunicados. Las empresas de información sobre riesgo de crédito están obligadas a proporcionar al afectado, gratuitamente, una copia de la información o datos personales usados para negar el crédito[338]. En el resto de los casos, la empresa está autorizada para cobrar una tarifa razonable.

Las agencias de información sobre riesgo de crédito están obligadas a investigar la veracidad de cualquier información que el afectado considere incorrecta o incompleta. Si resulta imposible corroborar la veracidad de los datos, las empresas deberán destruirlos, y si se comprueba que los datos son erróneos o incompletos, deberán ser corregidos.

Dado que son las empresas quienes toman la decisión final sobre estos asuntos, el afectado está autorizado legalmente a hacer incluir junto a la información registrada sobre su persona, una declaración sobre aquellos datos cuya

[338] La negativa o rechazo del crédito, debe ser justificada con los datos de la persona que se encuentran registrados en la base de datos de la empresa de riesgo de crédito.

veracidad el afectado pone en duda. Esta declaración deberá comunicarse, a partir de ese momento, a todas las personas a quienes sus datos se cedan.

1.3.- Seguridad

La legislación de EEUU es similar a la europea en relación con la exigencia legal de seguridad del tratamiento. Tanto las leyes federales como las estatales obligan al responsable del tratamiento a tomar las medidas necesarias para impedir cualquier acceso no autorizado a los datos y para impedir que los datos se usen para otros fines que los permitidos por la ley. El incumplimiento de esta obligación puede dar lugar a la responsabilidad civil de la empresa. Las empresas de información de crédito, en general, se caracterizan por tomar medidas de seguridad estrictas que impiden el acceso no autorizado a los datos personales sobre crédito o su posible manipulación. Procuran asimismo asegurar la integridad y seguridad de los datos durante todo el proceso de recolección de datos y procesamiento de datos.

2.- Bolivia

El Estado Plurinacional de Bolivia ha reformado su Constitución en el año 2009[339], oportunidad en la que ha incluido una nueva garantía constitucional de protección a la intimidad y a los datos personales, a la que denominó "acción de privacidad", sobre la cual profundizaremos a continuación. Probablemente por su reciente mutación constitucional, Bolivia todavía no ha desarrollado legislativamente el instituto de la protección de los datos personales en una ley específica. Por este motivo, ante la carencia de normas infra constitucionales, la protección genérica de la intimidad o la protección específica de los datos de carácter personal debe ser complementada por otras normas análogas o genéricas que indirectamente puedan hacer referencia al tema.

[339] Constitución del Estado Plurinacional de Bolivia, reformada en el año 2009. Fci.: http://bolivia.infoleyes.com/shownorm.php?id=469 (última consulta el 24/12/2011).

En este sentido, la Constitución Política del Estado de Bolivia[340] expresa en el Capítulo Tercero, referido a los Derechos Civiles y Políticos, Sección I sobre Derechos Civiles, artículo 21º: que "*Las bolivianas y los bolivianos tienen los siguientes derechos:* [...] *2. A la privacidad, intimidad, honra, honor, propia imagen y dignidad".*

Más adelante, la Carta Magna de Bolivia se ocupa nuevamente del derecho a la intimidad y en particular del derecho a la protección de los datos personales, en el Título IV referido a las Garantías Jurisdiccionales y Acciones de Defensa, en cuyo Capítulo Segundo dedicado a las Acciones de Defensa propiamente dichas, en su Sección III, se encuentra el artículo 130, que textualmente expresa:

"I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa".

A continuación el artículo 131 expresa que el procedimiento aplicable será el de la acción de amparo constitucional, y que en caso de que un juez o tribunal competente declare procedente la acción de privacidad, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado. Esta sentencia tiene efecto ejecutivo, ya que textualmente el apartado III del artículo 131 expresa: *"La decisión se elevará, de oficio, en revisión ante el Tribunal Constitucional*

[340] La Constitución Política de Bolivia es el decimoséptimo texto constitucional en la historia republicana de dicho país. Entró en vigencia el 7 de febrero de 2009, fecha en la que fue promulgada por el Presidente Evo Morales después de ser aprobada en un referéndum con un 90,24% de participación. La consulta fue celebrada el 25 de enero de 2009 y el voto aprobatorio alcanzó un 61,43% del total, es decir, 2.064.417 votos. El "no", por su parte, alcanzó 1.296.175 sufragios (es decir, un 38,57%). Los votos en blanco sumaron 1,7% y los nulos, un 2,61%.

Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución"[341].

La ley fundamental boliviana establece en el artículo 109 punto I, que "*Todos los derechos reconocidos en la Constitución son directamente aplicables y gozan de iguales garantías para su protección*", con lo cual queda claro que al estar el derecho a la protección de los datos personales reconocido en la Carta Magna, es de aplicación operativa y no programática, es decir que legalmente no requiere de una ley que lo desarrolle para su aplicación. Sin embargo, de *legeferenda*, proponemos la sanción de una leyespecífica sobre el tema.

El derecho a la intimidad también se encuentra contenido por la protección al secreto de la correspondencia y de los papeles privados, que la Constitución Política del Estado contempla en el art. 25 del texto reformado[342].

También el artículo 35 es muy claro al expresar que "*Las declaraciones, derechos y garantías que proclama esta Constitución no serán entendidas como negación de otros derechos y garantías no enunciados que nacen de la soberanía del pueblo y de la forma republicana de gobierno*". El artículo sigue la línea filosófica que entiende que al derecho no se lo construye, sino que se lo descubre. El derecho a la protección de los datos personales no es una creación posmodernista del derecho positivo, sino un descubrimiento basado en la necesidad humana de proteger su dignidad, libertad e intimidad de cada persona.

---

[341] La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme con lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la ley.

[342] Art. 25 de la Constitución Política de Bolivia (reformada en el año 2009): *"I. Toda persona tiene derecho a la inviolabilidad de su domicilio y al secreto de las comunicaciones privadas en todas sus formas, salvo autorización judicial. / II. Son inviolables la correspondencia, los papeles privados y las manifestaciones privadas contenidas en cualquier soporte; éstos no podrán ser incautados, salvo en los casos determinados por la ley para la investigación penal, en virtud de orden escrita y motivada de autoridad judicial competente. / III. Ni la autoridad pública, ni persona u organismo alguno podrán interceptar conversaciones o comunicaciones privadas mediante instalación que las controle o centralice. / IV. La información y prueba obtenidas con violación de correspondencia y comunicaciones en cualquiera de sus formas no producirán efecto legal".*

El derecho a la protección de datos personales existe aun cuando en Bolivia faltan leyes que desarrollen la Constitución, dada su calidad de derecho humano y personalísimo. Aun así, es conveniente su pronta incorporación en el derecho positivo infra constitucional para dar una mayor protección a los habitantes de Bolivia, a los efectos de que cuenten con garantías constitucionales y leyes específicas que protejan su intimidad y sus datos personales. También sería importante para las relaciones exteriores de Bolivia, ya que una incorporación legislativa seria y completa sobre este tema, le permitiría cumplir con las exigencias de una normativa equivalente requerida por la Unión Europea y otros Estados que se preocupan por este derecho. Una legislación que se precie de completa y seria sobre protección de datos personales, debe incluir la creación de un organismo de control o autoridad de aplicación en la materia.

Sin embargo, a pesar de la ausencia en Bolivia de una legislación específica sobre protección de datos personales y de una autoridad de control en la materia, cabe destacar que su texto constitucional es uno de los más modernos en la materia y más contundente al momento de expresar su protección.

3.- Brasil

La Constitución de la República Federativa de Brasil reformada en 1988[343] agregó a sus tradicionales garantías de mandato de seguridad y habeas corpus la acción de*habeas data*[344] en el artículo 5º numeral LXXII del capítulo I.

Esta es la primera de las constituciones que nombró con la denominación de *habeas data*[345] a una garantía constitucional concedida por los constituyentes para: "asegurar el conocimiento de informaciones relativas a la persona solicitante, que consten en registros de bancos de datos de entidades gubernamentales o de carácter

[343] Constitución de la República Federativa de Brasil; 1988.
Fci: http://www.georgetown.edu/pdba/Constitutions/Brazil/brazil88.html.
[344] El *habeas data* en Brasil ya contaba con antecedentes doctrinales, jurisprudenciales y legales; entre éstos últimos, la ley 824 del Estado de Río de Janeiro.
[345] Puccinelli, O. *El Habeas Data en Indoiberoamérica*. Editorial Temis. Bogotá, 1999, p. 295 y ss.

público", o "para la rectificación de datos cuando se prefiera hacerlo en proceso reservado (léase secreto) judicial o administrativo" (Art. 5º numeral LXXII).

Brasil incorporó en forma temprana el *habeas data* en su Constitución, motivos por los cuales su redacción es más limitada que el texto de las constituciones posteriores (Argentina, Perú, Venezuela, Colombia, Bolivia, etc.), y no garantiza el acceso a los bancos de datos privados[346]. Esta limitación en la regulación del instituto del *habeas data* en Brasil, es criticada, y a falta de una nueva reforma constitucional, será el Congreso o la jurisprudencia quienes deberán permitir el acceso a los bancos o registros de datos privados y avanzar con reglamentaciones más efectivas[347].

El primer párrafo del artículo Art. 5º numeral LXXII de la Constitución de Brasil, garantiza a quienes lo soliciten, el acceso a la información de carácter personal referido a su persona, existente en registros o bancos de datos públicos. La segunda parte concede al solicitante la facultad de rectificar un dato a él referido, mal consignado en los registros o bancos de datos públicos.

En el mismo artículo 5º y directamente relacionados con el instituto del *habeas data*, también se encuentran los numerales XXXIII y LXXVII.

El numeral XXXIII del artículo 5º, se refiere al *habeas data* impropio y textualmente expresa que "*todos tendrán derecho a recibir de los órganos públicos informaciones de su interés particular, o de interés colectivo o general, que serán entregadas en los términos que establezca la ley, bajo pena de responsabilidad, excepto aquellas cuyo secreto fuere imprescindible para la seguridad de la sociedad y del Estado*".

Por último, la Constitución contiene el numeral LXXVII del artículo 5º, que se refiere a la gratuidad del recurso de *habeas data*, y textualmente expresa que: "*Son gratuitas las acciones de habeas corpus y habeas data en la medida en que la*

[346] Quiroga Lavié, H. (2001). Op. cit., p. 13.
[347] Ibidem, p. 12.

ley disponga los actos necesarios para el ejercicio de la ciudadanía. 1) Serán de aplicación inmediata las normas definidoras de los derechos y garantías fundamentales. 2) Los derechos y garantías indicados en esta Constitución no excluyen otros que deriven del régimen y principios adoptados por ella o de los tratados internacionales en que la República Federativa del Brasil sea parte".

El régimen procesal del *habeas data* en el derecho brasileño es el mandamiento de ejecución (*mandato desegurança*), forma especial de proceso legislado en el 5º, numeral LXXI, para hacer efectivas las garantías constitucionales[348].

El mandamiento de ejecución debe ser concedido por los tribunales cuando falte una norma reglamentaria que torne viable el ejercicio de los derechos y libertades constitucionales y de las prerrogativas inherentes a la personalidad, la soberanía y la ciudadanía. Esta tutela constitucional obliga, en este caso, a los bancos o registros de datos tanto públicos como privados a ejecutar el *habeas data* aun a falta un procedimiento especialmente fijado por la ley.

El uso del mandamiento de ejecución no exige que se agote previamente la vía administrativa, ni requiere la existencia de abuso de autoridad, sino la mera existencia de la acción, aunque no haya violación de norma alguna, pero debe probarse la falta de interés o la morosidad manifiesta por parte del obligado en rectificar dicha situación.

De esta forma, y aun en la hipótesis de que no existiera la ley 9.507 (que más adelante analizaremos), la garantía constitucional del *habeas data* es plenamente operativa, ya que el "mandamiento de ejecución" es un instituto que se encuentra efectivamente vigente desde la sanción de la Constitución, y su posibilidad de interposición es absoluta e inmediata, conforme lo expresa el artículo 5, inc. II de la Constitución, según el cual, "las normas definidoras de los derechos y garantías fundamentales tienen aplicación inmediata".

[348] Ibidem.

La Constitución establece la gratuidad de la acción de habeas data (inciso LXVII, del art. 5º), junto a los actos necesarios para su ejercicio, en la medida en que la ley lo disponga.

Aun cuando la acción de habeas data de esta Constitución solo se refiere a la "rectificación" de los datos, la doctrina ha entendido que el objeto de la norma supone también la actualización, corrección y hasta la supresión de los mismos cuando ellos fueren incorrectos[349].En igual sentido, toda personatiene legitimación activa en el habeas data brasileño para poder que tomar conocimiento de todos los datos contenidos en bancos de datos relativos a su persona[350].

La legitimación pasiva del habeas data propio o tradicional (artículo 5º numeral LXXII) se dirige a "registros o Bancos de Datos de entidades gubernamentales o de carácter público", es decir que abarca tanto a aquellos bancos de datos de carácter público, como aquellos que tengan una función social de relevancia pública[351]. La legitimación pasiva del habeas data impropio del artículo 5º numeral XXXIII, recae en "entidades gubernamentales o de carácter público" que posean "registros o bancos de datos" en donde consten datos referidos al particular solicitante, o de interés colectivo o general.

En ambos incisos se limita la legitimación pasiva a los bancos de datos públicos, excluyendo a los bancos de datos privados. En el habeas data tradicional, regulado en segundo término (artículo 5º numeral LXXII), el sujeto pasivo de la garantía es quien tiene bajo su responsabilidad y custodia el banco de datos, con control sobre la información de personas físicas o jurídicas, y sobre la autoridad superior que deniega la exhibición o rectificación de la información contenida en el banco de datos.

En la doctrina brasileña se considera la acción contemplada en el instituto como un "interdicto de exhibición", por el cual se accede al contenido del "registro

[349] Ibidem.
[350] Puccinelli, O. (1999). Op. cit., p. 306.
[351] Ibidem, p. 309.

o banco de datos", y que propende a garantizar el derecho al conocimiento del contenido del mismo y a su "rectificación".

El art. 5º, numeral XXXIII, señala que toda persona tiene el derecho de "recibir de los organismos públicos las informaciones de su interés particular, o de interés colectivo o general, que serán brindadas en el plazo establecido por la ley, bajo pena de responsabilidad. Quedan exceptuadas aquellas cuya confidencialidad sea imprescindible para la seguridad de la sociedad y del Estado".

Se trata de dilucidar la contradicción entre una "información secreta", que justifica su existencia en función de imprescindibles razones de "seguridad de la sociedad y del Estado" y el principio de la "publicidad de los actos de gobierno", piedra angular de todo Estado democrático. El secreto deberá referirse a cuestiones que tengan la importancia indicada y, además, su mantenimiento debe ser "imprescindible" para el fin en cuestión. El límite estaría determinado por una ley que fije un plazo a partir del cual cesa la reserva. A falta de tal norma, será el juez quien determine, luego de oída la oficina gubernamental, la idoneidad del reclamo y la necesidad, o no, de la "confidencialidad" de la información.

La doctrina ha entendido que el *habeas data* funciona como tutela de los derechos colectivos en el apartado LXXIII del artículo 5º de la Constitución, el cual consagra la acción popular a favor de cualquier ciudadano para interponer un habeas data que tenga por objeto anular un acto lesivo al patrimonio público, o de una entidad donde participe el Estado, cuando estuviere afectada la moralidad administrativa, el medio ambiente o el patrimonio histórico y cultural, bajo la exigencia de identificar al autor, encontrándose la tutela exenta de costas judiciales[352].

[352] Quiroga Lavié, H. (2001). Op. cit., p. 12.

La ley Nº 9.507 de noviembre de 1997[353], desarrolló el instituto del habeas data regulando el derecho al acceso a informaciones y su trámite procesal. Esta ley[354] intentó corregir los defectos del texto constitucional, al declarar en su artículo 1º (luego vetado), de carácter público a todos los registros o bancos de datos que contengan informaciones que sean o puedan ser transmitidas a terceros o que no sean de uso privado de un órgano o entidad productora o depositaria de informaciones.

La ley también busca agilizar el proceso, estableciendo plazos muy cortos y prioridad sobre otros actos procesales (artículos 2º, 3º, 4º, 12º y19º), a los efectos de dar una reparación rápida al agravio sufrido por el afectado.

Como un requisito previo, la ley exige al interesado la presentación de una solicitud ante el banco de datos (art. 2º), el cual tiene un plazo de cuarenta y ocho horas para responderlo. En caso de que el interesado comprobara la inexactitud de algún dato relativo a su persona, podrá con la documentación comprobatoria, solicitar su rectificación (art. 4º). El banco de datos cuenta con diez días como máximo, contados desde la presentación de la solicitud para realizar la rectificación, e informar al interesado. Y aunque no se constate la inexactitud del dato, si el interesado presenta una explicación o contestación en la que justifique la relación entre los hechos sucedidos y los datos, tal información será anotada en el expediente o registro del interesado.

La ley define su objeto (art. 7º), al establecer que se concede el habeas data: 1º) para asegurar el conocimiento de informaciones relativas a la persona del solicitante, que consten en un registro o banco de datos de entidades gubernamentales o de carácter público. 2º) Para rectificación de los datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo. 3º) para

[353] La ley Nº 9.507 de Brasil sobre el derecho de acceso a informaciones y trámite procesal del habeas data. Esta Ley puede ser consultada en el CD-ROM anexo a la obra de Gozaíni, O. (2001). Op. cit.

[354] Ley Nº 9.507 de noviembre de 1997 (Brasil). Desarrolla el instituto del habeas data, regulando el derecho al acceso a informaciones y su trámite procesal.
Fci: http://www.dhnet.org.br/direitos/brasil/leisbr/acesso/habeasdata/

anotación en los asientos del interesado, de su contestación o explicación justificada en datos verdaderos relacionados con su situación judicial o acuerdo amigable.

La doctrina ha considerado novedosa la redacción del artículo 7º de la ley 9507, dado que agrega una tercera finalidad al instituto, que se suma a los dos clásicos objetivos constitucionales (toma de conocimiento y rectificación de datos). De esta forma, el inciso IIIº concede un nuevo *habeas data* para anotación en los asientos del interesado, para la contestación o explicación que este realice sobre datos verdaderos justificados, ya sea que estén en proceso judicial o en un proceso de acuerdo amigable. El espíritu de este inciso, es dar una nueva finalidad al instituto, para prevenir o reparar posibles agravios que pueda sufrir el titular de los datos como consecuencia de informaciones que aun siendo verdaderas, sean insuficientes para un análisis amplio, prestándose a una interpretación dudosa o errónea, sin una mayor explicación[355].

El *habeas data* recibe de la ley un tratamiento procesal prioritario (Art. 19º), al establecer textualmente que "los procesos de *habeas data* tendrán prioridad sobre todos los actos judiciales, excepto el *habeas corpus* y el mandato de seguridad (*mandato de segurança*)".

Al igual que la Constitución, la ley 9.507 reitera la gratuidad del procedimiento, (Art. 21º), expresando que son gratuitos los procesos administrativos de la acción de *habeas data* para el acceso a informaciones, rectificación de datos y anotación de justificación.

No fue legislada la transferencia internacional de datos, a pesar de la gran importancia de este tema.

La legislación sobre protección de datos personales en Brasil omitió crear una autoridad de control independiente que regule los registros y bancos de datos con facultades y potestades suficientes para dar protección efectiva a los datos personales.

[355] Puccinelli, O. (1999). Op. cit., p. 306 y ss.

Actualmente el parlamento brasileño se encuentra abocado a la discusión de un proyecto de ley de protección de datos personales, el cual tiene actualmente estado de anteproyecto presentado a la ciudadanía en consulta pública.

4.- Perú

Siguiendo el antecedente de la Constitución brasileña de 1988, la Constitución Política del Perú de 1993[356] incorporó la garantía constitucional del habeas data, la cual fue reformada en 1995 con modificaciones al art. 200, inc. 3º)[357], dentro del título que regula las Garantías Constitucionales. Los medios de comunicación y los organismos profesionales y gremiales del periodismo peruano plantearon su desacuerdo a la incorporación del habeas data, al entender que la norma constitucional atentaba contra la libertad de expresión[358].

El enunciado constitucional expresaba textualmente que: "*La acción de Habeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos que se refieren al artículo 2° incisos 5°, 6° y 7° de la Constitución*".

De esta forma, la Constitución peruana entendía que el habeas data era una garantía constitucional que venía a complementar los derechos del artículo 2° inciso 5° y 6°. Veamos su texto: Art. 2° - "*Toda persona tiene derecho a […] Inc. 5°, a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. El secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del fiscal de la*

[356] Infantes Madujano, P. *Constitución Política del Perú*. Editorial Librería y Ediciones Jurídicas. Lima, 1999, p. 137. Fci: http://www.georgetown.edu/pdba/Constitutions/Peru/peru.html.
[357] La Constitución Peruana de 1993 expresaba en su artículo 200 inc. 3º: "La acción de habeas data que procede contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona que vulnera o amenaza los derechos a que se refiere el artículo 2º, incisos 5º, 6º y 7º de la Constitución". Luego de la reforma de 1995, se excluyó al inciso 7º del artículo 2º.
[358] Ortecho Villena, V. (2002). Op. cit., p. 183.

Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado. Inciso 6°, *A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar*. Por último, el inciso 7° expresaba que toda persona tiene derecho "*al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propia. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que este se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley.*"

La doctrina de los autores había advertido que la acción de habeas data estaba mal concebida[359] en la norma contenida en el inciso 3) del artículo 200 de la Constitución de diciembre de 1993, en la medida en que también incluía como materia de protección los derechos contenidos en el inciso 7º[360] del artículo 2º de la misma carta fundamental, referente a las limitaciones a las libertades de información (otorgando el derecho a réplica), con la intención de proteger el honor, la buena reputación, la intimidad familiar, etc. Explica Víctor Ortecho Villena[361] que este habeas data contra la prensa no solo dio lugar a la temprana aplicación contra algunos medios de comunicación, sino que los demandados lo fueron ante el juez en lo penal, situación que luego se atemperó en alguna medida con la promulgación de la ley de aplicación de la acción constitucional dehabeas data Nº 26.301, el 2 de Mayo de 1994[362].

Estos sucesos dieron lugar a una larga campaña por parte de la prensa y demás medios de comunicación peruanos, para forzar la modificación de la

[359] Puccinelli, O. (1999). Op. cit., p. 71.
[360] El artículo 2º, inciso 7º, expresa textualmente que toda persona tiene derecho "al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propia. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que este se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley."
[361] Ortecho Villena, V. (2002). Op. cit., p. 189.
[362] Ley 26301 sobre la aplicación de la acción constitucional de habeas data (Perú). Fci.:http://www.bomberojuridico.com.ar/pagproductos/version_limitada/habeas_data/habeas_data_nuevo/legislacion/hd_ley_peru.htm

Constitución[363]. La enmienda constitucional se concretó y excluyó de la aplicación del habeas data al inciso 7º del artículo 2º y derogó el inciso b) del artículo 5º de la ley 26.301[364].

Luego de estas reformas, el habeas data en Perú dejó de afectar la libertad de prensa, siendo de aplicación al caso, el delito de difamación del Código Penal para aquellos actos abusivos de la prensa.

La garantía constitucional peruana de habeas data es una acción de naturaleza procesal, de procedimiento sumario que sirve para proteger los datos de las personas, y tiene directa relación con el artículo 1º de la mencionada Constitución de 1993, el cual expresa textualmente que "la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado".

Para asegurar el efectivo cumplimiento de los derechos mencionados el Título V de la Constitución legisla sobre las garantías constitucionales en tanto instrumentos procesales destinados a garantizar la vigencia efectiva de tales derechos fundamentales[365] expresados en los artículos 1º y 2º[366], por medio de la garantía procesal del *habeas data*[367].

En este sentido, el art. 200, inc. 3 del mencionado Título V se refiere a la acción de habeas data, como una garantía constitucional que procede contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refieren el art. 2, incisos 5 y 6, de la

[363] La ley 26470 del 12 de junio de 1995 convocó a la reforma constitucional que excluyó el inciso 7º del artículo 2º del radio de acción del *habeas data*.
[364] El inciso b) del artículo 5º de la ley 26.301 fue derogado por la ley 26545 del 10 de noviembre de 1995
[365] Infantes Madujano, P. (1999). Op. cit., introducción.
[366] Art.1º: [el reconocimiento de la persona como fin supremo de la sociedad y del Estado]; Art. 2º, inc. 1º [derecho a la vida y a su libre desarrollo y bienestar]; inc. 5º [derecho de información pública, secreto bancario y reserva tributaria]; inc. 6º [derecho a la intimidad: restricción de información].
[367] En concordancia con el art. 14 de la Convención Americana de Derechos Humanos y el artículo 31 inciso b) de la Ley Orgánica del Poder Judicial del Perú.

Constitución"[368]. Esta garantía fue incorporada por la Constitución de 1993, y reformada mediante la ley 26.470 del 12 de junio de 1995, siendo este el primer antecedente constitucional del instituto de la Protección de los Datos de carácter personal en Perú.

La doctrina ha entendido[369], que, si bien la reforma parece ampliar la garantía, de hecho, el constituyente la deja sujeta a las limitaciones que por razones de seguridad nacional disponga la ley, o a las razones que pueda discrecionalmente invocar el legislador a partir de la indiscriminada habilitación constitucional.

La garantía constitucional de habeas data, a su vez fue desarrollada en Perú por normas infraconstitucionales, como la ley 26.301[370] de mayo de 1994, "referida a la aplicación de las garantías constitucionales del *Habeas Data* y de la Acción de Cumplimiento", donde solamente trata cuestiones relacionadas con el juez competente y de forma procesal. Esta ley expresa su vocación de transitoriedad, ya que el artículo 1º expresa textualmente que: "En tanto se dicte la ley especial de la materia...", y reconoce la necesidad de un texto legislativo que aborde el tema con mayor profundidad luego de un debate parlamentario importante que trate a fondo cuestiones referidas al organismo o autoridad de aplicación, a la cesión de datos, a los datos sensibles, a los bancos de datos de información crediticia, etc.

El mencionado artículo 1º de la ley 26.301[371] indica que el juez competente es el Juez de Primera Instancia en lo Civil de Turno del lugar en donde tiene domicilio el demandante, o donde se encuentran ubicados los archivos mecánicos, telemáticos, magnéticos, informáticos o similares, o en el que corresponda al domicilio del demandado. A su vez, el artículo 5º de la ley 26.301 establece como

---

[368] Este texto fue luego modificado por la ley 26470 (12/06/95). Ver: Infantes Madujano, P. (1999). Op. cit., p. 138.
[369] Quiroga Lavié, H. (2001). Op. cit., p. 15.
[370] Modificada por la ley 26545 del 13/11/95, modificatoria de la ley 26301.
[371] Véase la ley 26301 en *Nueva Constitución Política del Perú. Comentada*. 1ª ed. Editorial Berrio. Lima (Perú), 2002, p. 105.
Esta ley también puede ser consultada en el CD-ROM anexo de la obra: Gozaíni, O. (2001). Op. cit.

requisito previo al inicio de las acciones judiciales, un requerimiento extrajudicial dirigido al demandado mediante notario público.

Sobre la legitimación activa [372] de la acción de habeas data, la Constitución Política del Perú no hace distingo entre personas físicas o jurídicas[373] (artículo 2º inciso 5º). Pero el artículo 1º de la ley 26.301 otorga legitimación activa, tanto a las personas naturales como a las jurídicas, públicas o privadas, a elección del demandante. El Defensor del Pueblo también goza de legitimación activa en defensa de los derechos constitucionales y fundamentales de la persona y de la comunidad (Art. 9º de la ley 26.520)[374].

La legitimación pasiva de la acción de habeas data se aplica contra la autoridad, funcionarios o personas particulares que tengan responsabilidad sobre registros, archivos o bancos de datos que estén bajo su orden, cuando se negaran a otorgar informes o datos a la persona que los solicite o a rectificar o cancelar esos datos.

La demanda se dirige contra la autoridad pública que se niega a proporcionar o contra la entidad pública o privada que tiene la información que afecta el derecho a la intimidad personal o familiar. Cuando el demandado no es una persona natural, la acción se planteará contra el representante legal de la autoridad, entidad o persona jurídica a la que se emplaza; y, cuando el agresor es el Estado, o funcionario público, su defensa correrá a cargo del Procurador General de la República con jurisdicción en el lugar.

El 28 de junio de 2001 fue publicada la ley 27.489[375], que regula las centrales privadas de Información de riesgos y de protección al titular de la información. En ella, se desarrollan conceptos como datos sensibles y bases de datos, entre otros.

[372] Es la persona facultada para interponer la acción de habeas data, agraviada por un acto de acción y omisión que vulnere sus derechos.
[373] Ortecho Villena, V. (2002). Op. cit., p. 182.
[374] Rodríguez Domínguez, E. *Derecho Procesal Constitucional*. 2ª ed. Editorial Jurídica GRIJLEY E.I.R.L. Lima,(Perú), 1999, p. 158.
[375] Ley 27.489, (Perú), publicada en el B.O. del 28/06/2001.

Pero la doctrina también ha criticado esta ley, por considerarla a la medida de las centrales o bancos de datos sobre riesgo de crédito. Es cuestionada la obligación de pago para ser excluido de una base de datos, junto a la inexistencia de un derecho a la reparación por error del titular del banco de datos.

El objeto establecido por el art. 200, inc.3º, es proteger a las personas frente al hecho u omisión por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refieren el art. 2º, inciso 5º (derecho de información pública, secreto bancario y reserva tributaria), e inciso 6º (derecho a la intimidad y restricción de información).

La Constitución no menciona al legitimado activo para iniciar la acción de *habeas data* (Art. 200 inc. 3º), pero por ser un instrumento procesal para proteger los derechos fundamentales de la persona, se entiende que estamos ante un derecho personalísimo, y por lo tanto la legitimación activa recae solo en las personas físicas.

La jurisprudencia peruana, a través de la Corte Suprema de Justicia, hizo lugar a un planteo de acción de *habeas data* interpuesta por una asociación civil contra la Dirección Nacional de Minería de Perú, por no haber brindado información sobre impacto ambiental, en la sentencia del 16 de junio de 1996[376]. Al hacer lugar a esta acción, la Corte peruana revocó la sentencia sostenida por las instancias inferiores en un caso en el que la Asociación Civil Labor solicitó a través de una acción de *habeas data* que se ordene al Director General de Minería que le proporcione información referente a los estudios de impacto ambiental presentados por la empresa *Southern Perú Copper Corporation* para el establecimiento de una planta de ácido sulfúrico dedicada a la fundación de cobre, junto a la resolución con la que se aprobaba la instalación de depósitos de ácido sulfúrico en el casco urbano de Puerto Llo. El fundamento legal sentado en la sentencia del Alto Tribunal peruano fue el inciso 5° del artículo 2° de la Constitución, antes mencionado y el

[376] Sentencia publicada en revista jurídica peruana La Ley, 1997-D-216. Obra citada por Quiroga Lavié, H. (2001). Op. cit., p. 16.

Código de Medioambiente. Al relatar los hechos, el fallo expresa que la Dirección General de Minería incumplió su obligación de proporcionar la información solicitada por la actora, haciendo hincapié en la necesidad de que los estudios de impacto ambiental puedan ser públicamente conocidos.

Entiendo que estamos ante una desnaturalización del derecho a la protección de los datos personales, dado que el objeto de la demanda y del fallo comentado es el derecho al acceso a la información, o bien como expresa Marcela Basterra, debemos entender que en el Perú se ha consagrado la acción de habeas data no solo para la protección de los datos personales, sino también para el efectivo ejercicio del derecho de acceso a la información pública[377].

Del artículo 200, inc. 3º, se desprende que el legitimado pasivo es cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refieren el art. 2, inciso 5º (derecho de información pública, secreto bancario y reserva tributaria), e inciso 6º (derecho a la intimidad: restricción de información), tanto por acción como por omisión.

La Constitución no establece sanción para el legitimado pasivo, ya que en caso de que fuere considerado responsable del agravio denunciado, el demandado sólo puede ser condenado al pago de costas a la parte vencedora.

Para solicitar el pago de una indemnización por daños y perjuicios, la persona agraviada deberá plantear una acción civil en la cual las violaciones a su derecho a la intimidad y a la protección de datos personales, queden demostradas y probadas[378].

El Ministerio de Justicia de Perú, por medio de la Resolución Nº 094-2002-JUS de marzo de 2002, ha creado una Comisión Especial encargada de proponer el Proyecto de Ley de Protección de Datos Personalesy elaborar las propuestas legislativas y administrativas que correspondan. Sería acertado que la comisión

[377] Basterra, M. (2008). Op. cit., p. 274.
[378] Ortecho Villena, V. (2002). Op. cit., p. 189.

formada tenga a la vista la legislación chilena y argentina, junto con la opinión de la doctrina para que su propuesta evite repetir los errores cometidos por las leyes mencionadas.

La doctrina no compartió la decisión del Ministerio de Justicia de integrar, la mencionada comisión, con funcionarios del Sistema Nacional de los Registros Públicos[379], dado que no tienen relación con los datos personales, excluyendo a representantes de entidades públicas vinculadas a la administración y privacidad de datos personales.

En la ley 27.489 podemos encontrar que los titulares de la información, personas naturales o jurídicas a quienes se refiere la información, tendrán los derechos al acceso, a la modificación, a la cancelación y rectificación. Define cuáles son los bancos y las bases de datos comprendidas, los tipos de datos y realiza observaciones especiales[380].

5.- Nicaragua

La Constitución de la República de Nicaragua todavía no ha incorporado en forma expresa la acción de protección de los datos personales. De todas formas, como todas las Cartas Constitucionales americanas, protege al derecho a la intimidad. Su artículo 26º expresa textualmente que "Toda persona tiene derecho a su vida privada y a la de su familia", con lo cual es posible interpretar que el derecho a la intimidad en general se encuentra expresamente protegido por la constitución nicaragüense y en forma indirecta podemos extender esta protección a los datos personales y al derecho a la autodeterminación informativa, conforme a las teorías de las esferas explicada en el capítulo primero de estos estudios.

[379] Referidos a la inscripción de vehículos, prendas agrícolas o industriales, propiedad inmueble, buques, embarcaciones pesqueras, aeronaves, minería, personas jurídicas, etc., y personas naturales (mandatos y poderes, testamentos, sucesiones intestadas, personal, comerciantes).
[380] Basterra, M. (2008). Op. cit., p. 276.

Cierto es que tampoco ha sido sancionada en Nicaragua una ley específica sobre protección de datos personales, pero sí existe una ley sobre acceso a la información pública, clasificada con el número 621[381], dentro de la cual se encuentra una definición sobre *habeas data* y algunas reglamentaciones procedimentales. No compartimos esta técnica legislativa de reiterado uso en Latinoamérica, por la confusión que genera entre dos institutos diferentes que protegen derechos también diferentes: el derecho al acceso a la información pública y el derecho a la protección de los datos personales. Existen entre estos dos derechos grandes diferencias esenciales; así, mientras el derecho a la protección de datos personales se desarrolla en un ámbito que puede ser de naturaleza tanto pública como privada con respecto a los datos del individuo, se refiere a información sobre sí mismo y es un derecho personalísimo o individual, aun cuando pueda interponerse contra bases o bancos de datos tanto públicos como privados para conocer y controlar datos personales existentes en esas centrales de datos. Por el contrario, el derecho al acceso a la información pública se desenvuelve sólo en un ámbito público, ya que se refiere a información o datos de carácter público y es un derecho colectivo, porque se ocupa de proteger un bien colectivo que pertenece a la cosa pública.

Como mencionamos antes, la ley nicaragüense de acceso a la información pública define al*habeas data* en el art. 4º inc. b) diciendo que es una: *"garantía de tutela de los datos personales privados asentados en archivos, registros, bancos de datos u otros medios técnicos, sean estos públicos o privados, cuya publicidad constituya una invasión a la privacidad personal o familiar, que tenga relevancia con respecto a datos sensibles de las personas, su vida íntima, incluyendo sus asuntos familiares, que se encuentren en poder de las entidades especificadas en el art. 1º. Se entiende por datos sensibles, los datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliaciones políticas, sindicales e información referente a la salud física y psicológica o a la actividad íntima de las personas, en cualquier formato en el que*

[381] Ley Nº 621 de Nicaragua, publicada en La Gaceta Nº 118 del 22/06/2007.

se generen o almacenen. De igual manera el habeas data garantiza el acceso a toda persona a la información que puede tener cualquier entidad pública sobre ella, así como el deber a saber por qué y con qué finalidad tienen esa información".

De esta definición se desprende que la ley de Nicaragua asigna legitimación activa en materia de protección de datos personales para interponer un *habeas data* a *"toda persona",* de lo cual, a falta de mayor precisión podríamos entender que abarca sólo a las personas físicas. Con respecto a la legitimación pasiva, la legislación nicaragüense adopta un criterio amplio al indicar que se encuentran incluidos aquellos que almacenen datos personales, sean instituciones públicas, sociedades mixtas, subvencionadas por el Estado o entidades privadas que administren o reciban recursos públicos, concesiones, beneficios fiscales u otros privilegios.

Con respecto a los derechos que la ley otorga a los titulares de los datos, la ley reconoce el derecho de acceso a la información que sobre el titular exista en los bancos de datos públicos, así como la finalidad con la cual fue recabada. En este punto surgen en forma patente la necesidad de una ley específica para proteger a los datos personales, ya que como consecuencia de la confusión de institutos con el derecho de acceso a la información pública, ya que el *habeas data* queda restringido sólo a los bancos de datos públicos y ha excluido a los bancos de datos privados.

Con respecto a los datos sensibles, es acertada la descripción que realiza la ley sobre esta categoría de datos personales, pero la ley omite prohibir su recolección, cuestión que es el sentido de la clasificación legal, dado el potencial discriminatorio que tienen estos bancos de datos. En tal sentido, el derecho comparado es prácticamente unánime al prohibir la existencia de los bancos de datos sensibles, salvo expresas excepciones.

El sistema legal nicaragüense no ha legislado todavía sobre el procedimiento judicial, sobre los derechos a actualizar, rectificar, eliminar o cancelar los datos de un banco de datos, sobre otros derechos de los titulares de los datos, las

obligaciones de los usuarios y responsables de los bancos de datos y lo más importante: la creación de un órgano de control que actúe como autoridad de aplicación en materia de protección de datos personales y aplique las sanciones que correspondan. En esta materia, Nicaragua tiene la oportunidad de ser novedosa en el continente americano, en el caso de que llegara a diseñar un órgano de control independiente y autónomo del Poder Ejecutivo del Estado.

En función de lo expresado *ut supra*, y a pesar de considerar a la legislación existente en Nicaragua insuficiente para la protección efectiva de los datos personales y de la autodeterminación informativa, siendo necesaria la promulgación de una ley específica en la materia, la acción de protección de datos personales podría ser interpuesta en Nicaragua, aun cuando no esté expresamente mencionada en su Constitución. A esta tesis abonan la protección genérica de la intimidad contemplada en la Constitución, la ley antes mencionada y los convenios internacionales en los que Nicaragua forma parte.

6.- Panamá

Panamá buscó dar protección jurídica a los datos de carácter personal, primero por medio de la legislación, con la ley 6/2002 Nº 24.476 del 23/01/2002 y recién dos años más tarde con la incorporación de la acción de *habeas data* en su Constitución. Analicemos primero la norma constitucional.

La Constitución de Panamá incorporó la acción de *habeas data* luego de ser reformada en el año 2004. Se encuentra en el artículo 44, cuyo texto expresa: "Toda persona podrá promover acción de habeas data con miras a garantizar el derecho de acceso a su información personal recabada en bancos de datos o registros oficiales o particulares, cuando estos últimos pertenezcan a empresas que prestan un servicio al público o se dediquen a suministrar información. Esta acción se podrá interponer, de igual forma, para hacer valer el derecho de acceso a la información pública o de acceso libre, de conformidad con lo establecido en esta Constitución. Mediante la acción de *habeas data* se podrá solicitar que se corrija, actualice, rectifique, suprima

o se mantenga en confidencialidad la información o datos que tengan carácter personal. La ley reglamentará lo referente a los tribunales competentes para conocer del *habeas data*, que se sustanciará mediante proceso sumario y sin necesidad de apoderado judicial".

La Constitución panameña ha reunido en un mismo artículo, dentro de la acción de habeas data, a los derechos a la protección de los datos personales y al acceso a la información pública. Como ya comentamos en otros puntos de este estudio, consideramos que esta técnica legislativa es criticable, dado que genera confusión a ambos institutos, cuestión que podría haber sido evitada simplemente con la incorporación de un artículo diferente para cada acción o garantía constitucional. Al momento del desarrollo legislativo y reglamentario, Panamá tendrá la oportunidad de solucionar este problema por medio de dos leyes independientes para cada derecho. Por lo pronto, cabe destacar la importancia que otorga al *habeas data* su jerarquía constitucional en el sistema legal panameño.

La Constitución panameña parece dar legitimación activa sólo a las personas físicas, dado que se refiere en su texto a "toda persona", sin especificar nada sobre las personas jurídicas o ideales. La legislación de desarrollo de la constitución adopta un criterio amplio al interpretar que por "toda persona" debe entenderse a cualquier persona, sea natural, jurídica o de existencia ideal.

Con respecto a la legitimación pasiva, la Constitución panameña es muy completa al establecer que procederá la acción de *habeas data* tanto contra bancos de datos públicos como privados que presten un servicio al público o estén destinados a proveer informes. El artículo 42º establece que "toda persona tiene derecho a acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la ley. Esta información sólo podrá ser recogida para fines específicos, mediante consentimiento de su titular o por disposición de autoridad competente con fundamento en lo previsto en la ley.

El precepto constitucional establecido en el artículo 44 otorga diferentes derechos al titular del dato personal: derecho de acceso, de corrección, de actualización, rectificación, supresión y confidencialidad de la información referida a su persona. Además, el artículo 42º establece la obligatoriedad de que el titular de los datos preste su consentimiento para que el responsable del banco de datos pueda realizar el tratamiento de ellos, o bien que exista una orden de autoridad competente que autorice la recolección de datos personales.

Pasando a analizar la legislación panameña sobre el tema, como ya mencionamos, la ley 6/2002 establece, con respecto a la legitimación activa, un criterio amplio, dado que en el artículo 1º inciso 9º, expresa que se entiende por "persona", a "Cualquier persona, ya sea natural o jurídica, que actúe en nombre propio o en nombre de un tercero".

Sobre la legitimación pasiva o bancos de datos comprendidos, la acción de habeas data procede en la ley 6/2002 cuando el funcionario público o titular o responsable del registro, archivo, o banco de datos en el que se encuentra la información o dato personal reclamado, no le haya suministrado lo solicitado o lo haya hecho de manera insuficiente o en forma inexacta. Es decir, que en la mencionada ley la acción de *habeas data* pareciera a priori que no procede contra bancos de datos de titularidad privada. Sin embargo, más adelante el artículo 2º *in fine* expresa que: "Las empresas privadas que suministren servicios públicos con carácter de exclusividad, están obligadas a proporcionar la información que les sea solicitada por los usuarios del servicio, respecto a este". Es decir que la acción de *habeas data* procede tanto contra archivos, registros o bancos de datos tanto públicos como aquellos que son de titularidad privada y suministran servicios públicos.

La legislación panameña no contempla, por ejemplo, la legitimación pasiva de los bancos de datos privados destinados a proveer informes. Esto es contradictorio, ya que uno de los efectos más buscados con la inclusión del *habeas data* en las constituciones americanas, fue garantizar el control por parte de las

personas sobre su información personal, incluso su actualización y veracidad. En Argentina el principal uso que se dio al *habeas data* y a la ley de protección de datos personales 25.326, fue el control de la información que ofrecen los bancos de datos de informes sobre riesgo de créditos.

La acción de *habeas data* panameña requiere como requisito previo para su procedencia el agotamiento de la instancia prejudicial. Esta exigencia previa para acceder a la instancia judicial es coherente con los principios de economía procesal y celeridad del proceso judicial. En caso contrario, esta acción puede llegar a desvirtuarse y congestionar los despachos judiciales con trámites burocráticos que en muchos casos pueden encontrar rápida solución con la sola presentación ante el responsable del archivo o banco de datos. Sin embargo, entiendo que la falta de respuesta por parte de banco de datos, que obligue al titular del dato personal a recurrir a la justicia, debería generar una sanción pecuniaria en contra del responsable del banco de datos, de forma tal que desaliente todo tipo de especulación y cálculo al respecto.

En la misma norma referida al *habeas data*, en el capítulo IV, la ley establece exigencias para la recolección de datos: prohíbe a los agentes del Estado divulgar información confidencial, datos contenidos en los registros individuales o expedientes de personal o de recursos humanos de los funcionarios, y establece un tratamiento especial para la información de acceso restringido, la cual, como veremos, no se refiere a datos de carácter personal, sino a información del Estado que este podría clasificar como secreta. Una vez más observamos en este caso una confusión de institutos: *habeas data* con acceso a la información con secretos oficiales. Cada uno de estos institutos debería tener su propia ley para no confundir a las personas.

En tal sentido, en forma taxativa, en su artículo 14º, la ley panameña considera de acceso restringido a la información: a) relativa a la seguridad nacional; b) relativa a secretos comerciales o a información comercial de carácter confidencial, obtenida por el Estado como consecuencia de su actuación en la

regulación de actividades económicas; c) relativa a procesos judiciales o jurisdiccionales adelantados por el Ministerio Público y el Órgano Judicial (información sólo accesible para las partes del proceso hasta tanto el proceso se encuentre ejecutoriado); d) relativa a procesos de investigación impulsados por el Estado y sus diversos organismos centralizados o descentralizados (el art. 14º inc. 4º detalla a tales organismos); e) relativa a la existencia de yacimientos minerales y petrolíferos; f) memorias, notas, correspondencia y documentos relacionados a negociaciones diplomáticas, comerciales e internacionales de cualquier índole; g) documentos, archivos y transcripciones recibidas de otros Estados en investigaciones penales, policiales o de otra naturaleza; h) las actas, notas, archivos y otros registros o constancias de las discusiones o actividades del Consejo de Gabinete del Presidente o del Vicepresidente de la República, con excepción de aquellas correspondientes a discusiones o actividades relacionadas con las aprobaciones de los contratos; i) la transcripción de las reuniones e información obtenida por las comisiones de la Asamblea Legislativa, cuando se reúnan en el ejercicio de sus funciones fiscalizadoras para recabar información que podría estar incluida en los puntos anteriores.

La ley panameña establece un lapso de diez años durante los cuales la información de acceso restringido, enumerada en el párrafo anterior, no podrá ser divulgada. Este plazo legal muestra a las claras que la información de acceso restringido no se refiere a datos de carácter personal, puesto que al ser el control un derecho personalísimo del titular del dato, el Estado no podría establecer un plazo para su divulgación, y si lo hiciera estaría lesionando el derecho a la autodeterminación informativa.

Por último, con respecto al procedimiento judicial, la ley establece que los Tribunales Superiores que conocen de la acción de amparo a las garantías constitucionales (si el responsable del banco de datos fuera un funcionario jerárquico municipal o provincial), serán competentes para entender en una acción de *habeas data*. Para aquellos casos en los que el responsable del banco de datos

fuera un funcionario con jurisdicción en más de una provincia, o en toda la República de Panamá, la acción de *habeas data* será competencia de la Corte Suprema de Justicia.El procedimiento asignado por la ley a la acción de *habeas data* en Panamá es el sumario, sin mayores formalidades y siguiendo el rito establecido para la acción de amparo.

7.- Canadá

La ley de Protección de la Información Personal y de los documentos electrónicos[382] (conocida como la ley PIPEDA, Bill C-6) fue sancionada en Canadá el 13 de abril de 2000 y entró en vigencia el 1 de enero de 2001. Recientemente esta ley federal canadiense fue reformada en abril del año 2011, luego de un largo debate iniciado en el año 2008 sobre una reforma general a esta legislación de protección de datos personales canadiense y para ello la Oficina del Comisionado de Privacidad de Canadá, así como las comisiones pertinentes del Parlamento elaboraron sendos informes a partir de los cuales se sancionó la reforma[383].

La ley vigente legisla sobre la protección de datos personales y otorga nuevos derechos a las personas físicas para que puedan protegerse de la acumulación, uso o revelación (*disclosure*) de la información personal en la actividad comercial del sector privado. Canadá intentó alcanzar, con esta ley, los estándares jurídicos europeos para la protección de datos personales.

Antes de la entrada en vigencia de la Ley de Protección de la Información Personal y de los documentos electrónicos (2001), la provincia de Quebec era el único Estado en América del Norte que cumplía con los niveles de protección jurídica exigidos por la Unión Europea.

---

[382] Véase el siguiente sitio web sobre la PIPED *Act.*. Fci: http://en.wikipedia.org/wiki/Personal_Information_Protection_and_Electronic_Documents_Act

[383] Véase el contenido actualizado de la ley canadiense de privacidad (Ley de Protección de Información Personal y de los Documentos Electrónicos); SC 2000, c. 5; actualizada al 18/01/2012, con la reforma del 01/04/2011 en el sitio web del Departamento de Justicia de Canadá: www.justice.gc.ca

La ley regula la recolección, uso y revelación de información personal tanto en el sector público como privado. Establece derechos que hacen que el sistema sea más transparente y responsable.

La norma crea un código de información justo para garantizar una mayor protección jurídica de los datos de carácter personal que usa y procesa el gobierno. De esta forma, la ley otorga mayor control a los individuos en cuanto al derecho para examinar la información sobre ellos en secciones gubernamentales federales y agencias, determinando algunas excepciones específicas. Los individuos tienen derecho a corregir cualquier error y ante la negativa del banco de datos, pueden requerir que un agregado se adjunte a la información que describa cualquier corrección pedida no realizada.

Las personas pueden interponer estas facultades ante una gran diversidad de archivos federales del gobierno, tales como los archivos de pensión, de seguros de desempleo, de impuestos, de despachos de aduanas, de seguridad, de préstamos de estudiantes y militares.

El gobierno federal tiene límites, impuestos por la ley, en sus posibilidades de recolección de información personal. Tiene la obligación de solicitar, en lo posible, los datos en forma directa de la persona afectada. Se exige que se comunique a la persona cuando la información está siendo reunida y cómo se usará. Se prohíbe el uso de la información para otros propósitos que no sean permitidos por la ley. También se impide que se guarde la información por mucho tiempo y permite obtener el acceso a la persona asegurando que la información sea exacta, a la fecha y lo más completa posible. Los archivos de datos tienen prohibido divulgar la información personal, a menos que sea específicamente permitido por esta u otra ley.

La autoridad de control y aplicación en materia de protección de datos personales de Canadá es la Oficina del Alto Comisionado de Privacidad[384]. Esta oficina se encuentra a cargo de un funcionario del Parlamento, que reporta directamente a la Cámara de los Comunes y el Senado[385]. La Oficina del Alto Comisionado de Privacidad de Canadá ha supervisado una serie de importantes investigaciones y auditorías de las prácticas de manejo de la información personal de los sectores público y privado. Ella fue la autoridad de protección de datos que por primera vez en el mundo llevó a cabo una investigación exhaustiva de las políticas y prácticas de privacidad de la popular red social, Facebook.

Canadá tiene dos leyes federales de privacidad; la Ley de Privacidad (*The Privacy Act*) y la Ley de Protección de Información Personal y de Documentos Electrónicos. La Ley de Privacidad[386] entró en vigor el 1 de julio de 1983. Esta ley impone obligaciones a los departamentos del gobierno federal, constituido por cerca de 250 agencias encargadas de hacer respetar los derechos de privacidad de las personas al limitar la recopilación, uso y divulgación de información personal. La Ley de Privacidad da a los individuos el derecho de acceder y solicitar la corrección de la información personal sobre ellos mismos.

La Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA), establece reglas de juego para las organizaciones del Sector Privado que recogen, utilizan o divulgan información personal en el curso de sus actividades comerciales. La ley da a los individuos el derecho de acceder y solicitar la corrección de la información personal que puedan haber recogidolas organizaciones.

Inicialmente la Ley PIPEDA fue sólo aplicable a la información personal sobre clientes o empleados, recogida, utilizada o revelada en el curso de los

[384] La Oficina del Alto Comisionado de Privacidad de Canadá cuenta con un sitio web oficial cuya dirección en Internet es la siguiente fci.: http://www.priv.gc.ca/index_e.asp.
[385] Actualmente esta oficina se encuentra a cargo de Jennifer Stoddart.
Fci:: http://www.priv.gc.ca/au-ans/bio_e.asp .
[386] La Ley de Privacidad de Canadá (*Privacy Act*) puede ser consultada en el siguiente sitio web fci.: http://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html#h-1.

negocios realizados por el sector privado que estuvieran regulados federalmente: por ejemplo, organizaciones como bancos, aerolíneas y compañías de telecomunicaciones. Actualmente, la ley alcanza también a la información personal recopilada, utilizada o revelada por el sector minorista, las empresas editoriales, la industria de servicios, fabricantes y otros organismos con regulación provincial no federal, pero no es aplicable a la información personal de los empleados de estos organismos sometidos a regulación provincial.

Aun cuando muchas provincias canadienses tienen sus propias leyes sobre privacidad en el marco del sistema federal de gobierno, estas leyes son sustancialmente similares a la ley federal. La ley PIPEDA se sigue aplicando en las provincias en el sector privado regulado por el gobierno federal y en lo referente a la información personal en las transacciones inter-provinciales e internacionales realizadas por todos los organismos que realicen tales actividades comerciales.

Columbia Británica, Alberta y Quebec son provincias con leyes muy similares a la ley federal PIPEDA en lo referido a la recolección, uso y divulgación de información personal por empresas y otras organizaciones e individuos, con un derecho general de proporcionar el acceso y corrección de la información concerniente al titular del dato. Ontario ha aprobado recientemente una ley de privacidad para proteger la información médica personal que sigue los lineamientos generales de la ley federal. Otras provincias también han aprobado leyes para tratar específicamente la recolección, uso y divulgación de información personal de salud por proveedores de servicios médicos y otras organizaciones de atención de salud.

También existen regulaciones provinciales y federales sobre protección de datos personales en leyes específicas sectoriales que se refieren sólo a una actividad o sector determinado: por ejemplo, la ley federal sobre el sector bancario contiene disposiciones que regulan el uso y divulgación de información personal por las instituciones financieras reguladas por el gobierno federal.

La mayoría de las legislaciones provinciales sobre derechos del consumidor, se ocupan de proteger a las personas ante los bancos de datos de informes sobre riesgo de crédito, para garantizar la exactitud de la información, los límites a la divulgación de la información y el derecho de dar a los consumidores el acceso y rectificación o cancelación de sus datos personales. Hay también un gran número de leyes provinciales que contienen disposiciones sobre obligaciones de confidencialidad en materia de información personal recopilada por profesionales.

8.- Colombia

Desde la década de 1980encontramos antecedentes colombianos en materia de derecho a la protección de datos personales:

En 1986, la Universidad de los Andes elaboró un proyecto de ley de datos personales que sirvió de antecedente para proyectar una iniciativa parlamentaria de perfil permisivo sobre habeas data. Este proyecto parte de la licitud de construir bancos de datos de información personal, previa condición de ser comunicados a una autoridad de control, y tiene como objeto la tutela, por vía de un desarrollo legislativo, de los datos de las personas físicas y jurídicas frente a bancos de datos personales públicos y privados, ya sean manuales o informáticos.

En 1987, (cuatro años antes de ser sancionada la Constitución Política de Colombia de 1991) entraba en vigencia el Código Procesal Penal, que también abordaba la protección de la intimidad, dado que además de habilitar el uso de una acción de tutela y protección de las informaciones existentes en los bancos de datos, autoriza a los interesados a apelar a medidas procesales equivalentes en el marco de un proceso contencioso y a solicitar judicialmente el conocimiento, la actualización o rectificación de un banco de datos, puesto que el derecho a la información es de aplicación inmediata en Colombia .

Finalmente se consagra el derecho a la protección de los datos personales garantizado por el *habeas data* en la Constitución Política de la República de

Colombia del año 1991[387] (luego reformada en diferentes oportunidades, siendo su última enmienda en el año 2005[388]). En esta norma fundamental colombiana se consagró la protección de los datos de carácter personal en su art. 15. Posteriormente, en el año 2003, el texto del artículo fue modificado y quedó redactado de la siguiente forma:

ARTICULO 15 (Constitución Política de Colombia): *Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.*

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar.

---

[387] Galvis Gaitán, F. *La Constitución explicada por los constituyentes*. Editorial Temis; Santa Fe de Bogotá (Colombia); 1991, p. 6.

[388] Para consultar el texto vigente de la Constitución Política de la República de Colombia, véase el sitio web del Senado de Colombia. Fci.: www.senado.gov.co
http://pdba.georgetown.edu/constitutions/colombia/col91.html

Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley. (Modificado por Acto Legislativo Número 2 de 2003).

El constituyente buscó proteger una zona de reserva o intimidad de las personas que se extiende a su familia, y ordena que sea resguardada por el Estado y por el derecho.

Encontramos que la primera parte, del artículo 15º de la Constitución, es redundante y desafortunado al asociar el derecho a la intimidad con el derecho al buen nombre, ya que en la misma Carta Magna, en el artículo 21º, se protege el derecho a la honra entre los derechos fundamentales .

La segunda parte del párrafo primero del artículo 15º de la Constitución, consagra el derecho a la información. No prohíbe la existencia de bancos de datos, sino que busca garantizar a las personas el acceso a los mismos, la posibilidad de rectificarlos y de actualizarlos.

La Constitución busca garantizar que en los procesos de recolección de datos se respete la libertad y demás garantías constitucionales. El segundo párrafo del artículo 15º expresa textualmente que en el tratamiento y circulación de datos se respetará la libertad y demás garantías consagradas en la Constitución.

El inciso tercero y el cuarto del artículo 15º contienen dos grandes hipótesis:

1) La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial (régimen represivo de la libertad) en los casos y con las formalidades que establezca la ley;

2) Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados en los términos que señale la ley. Pues

bien, aquí no se requiere orden judicial, se autoriza un régimen preventivo de la libertad. En este sentido, para efectos judiciales la naturaleza propia de la función lleva a que, para recolectar pruebas, la orden sea impartida por un Juez. Para efectos tributarios, en los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, por las autoridades administrativas correspondientes, en los términos que señale la ley. Función de todos modos reglada, ya que no existe un poder discrecional autorizado en este régimen preventivo atenuado, para que el Estado o la administración pública puedan exigir libros de contabilidad a los particulares. Como podemos observar, la Constitución de 1991 ya garantizaba a las personas el derecho de conocer, actualizar y rectificar las informaciones que se hallan recogidas sobre ellas en bancos de datos y en archivos de entidades públicas o privadas. Ya disponía, también, que en la recolección, tratamiento y circulación de datos se respetara la libertad y demás garantías constitucionales. Sin embargo, es criticable la técnica constitucional colombiana, dado que regula en el mismo artículo el derecho a la intimidad, el *habeas data* y la inviolabilidad de los documentos privados.

La Corte Constitucional de Colombia[389], en diferentes sentencias establece que, dependiendo de la naturaleza de cada derecho fundamental en concreto, las personas jurídicas pueden ser titulares activos de derechos fundamentales. En este sentido, la legitimación activa del *habeas data* se extiende también a las personas jurídicas o ideales.

Con respecto a la legitimación pasiva, surge de la Constitución de Colombia que los sujetos obligados son aquellas personas naturales o jurídicas, públicas o privadas que posean bancos de datos personales con el fin de poner en circulación los datos que almacenan, o con aptitud de hacerlo y de generar información a terceros.

El marco jurídico de la protección de datos personales en Colombia se estructura desde la Constitución (art. 15°) que establece al *habeas data* como un

[389] Corte Constitucional de la República de Colombia. Fci.: http://www.corteconstitucional.gov.co/.

derecho fundamental y con una serie de normas o leyes sectoriales que indirectamente se refieren a la materia. A ello se suma la importante jurisprudencia de la Corte Constitucional, que desde 1992 se ha venido pronunciando en cientos de sentencias.

El Congreso de Colombia[390] tramitó, en el año 2003, un proyecto de Ley Estatutaria con disposiciones para la protección de datos personales y regulaciones sobre la recolección, tratamiento y circulación de estos datos. El origen de esta iniciativa surgió como consecuencia de una presentación de la Defensoría del Pueblo de Colombia ante el Senado de la República.

Finalmente, en el año 2007, se promulgó la ley 221/2007, que desarrolla al artículo 15 de la Constitución Política de Colombia y establece una regulación legal infra constitucional a la protección de los datos de carácter personal.

La ley establece expresamente que su objetivo es garantizar el *habeas data*, contempla una serie de regulaciones que integran principios de orden constitucional y del derecho comparado. Parte de la consideración de que las personas son titulares de sus datos y por tanto las únicas habilitadas para autorizar su entrega y determinar la finalidad de su tratamiento y circulación. Como consecuencia, establece que es necesario el consentimiento previo, escrito e informado del titular de los datos, para que sea procedente el tratamiento. Asimismo, el consentimiento puede ser revocado por el titular de los datos.

Como derivación del respeto debido a la honra y buen nombre que deben primar en el tratamiento de datos por disposición del artículo 15 de la Constitución, se consagra el principio de Calidad de los Datos, en virtud del cual, estos deben ser veraces, actuales, proporcionados, imparciales, completos y comprobables, entre otras características; igualmente, los datos deben ser tratados para el fin que contempla la autorización del titular.

[390] Datos sobre el proyecto de ley sobre protección de datos de carácter personal, pueden ser encontrados en el sitio web del Senado de Colombia, bajo el Nº de proyecto 64/2003 (http://www.senado.gov.co/Senado/senadoa.htm) y publicado en la Gaceta 411 del 2003.

Los datos negativos deben ser suprimidos o caducados una vez transcurrido el término que la ley contempla para los diversos eventos, es decir, cinco años cuando el pago se produce como consecuencia de un proceso ejecutivo, dos años cuando el pago se realiza de manera voluntaria y hasta el doble de la mora cuando ésta haya sido inferior a un año.

Existen en esta ley sendos capítulos que regulan los deberes de los titulares de los datos, de los usuarios y de los responsables del tratamiento. Además, un capítulo de Derechos y Garantías que desarrollan de manera integral los Derechos de Acceso y Habeas Data, entendidos como la posibilidad de solicitar y obtener información acerca de la existencia de un tratamiento de datos referidos a la persona interesada y, subsecuentemente, solicitar y obtener la actualización, rectificación, bloqueo o supresión de los mismos cuando a ello hubiere lugar. Otra garantía está representada por la posibilidad de acudir a la Defensoría del Pueblo para hacer efectivos, mediante el amparo informático, los derechos de que es titular. Finalmente, la persona tiene derecho a ser notificada por la fuente de información, cuando quiera que se vaya a hacer un reporte de datos negativos que le conciernen.

Los bancos de datos deben ser autorizados para operar por el ente de vigilancia y control, en éste caso, la Defensoría del Pueblo, previo el cumplimiento de algunos requisitos que acrediten la idoneidad técnica, logística y administrativa para realizar las actividades propias del tratamiento de datos. El proyecto dispone igualmente la creación de un Registro Nacional Público de Bancos de Datos, cuyo manejo y gestión se encomienda también a la Defensoría.

Se ha contemplado el procedimiento de Amparo Informático, de naturaleza sumaria e informal, que permite a los titulares de los datos recurrir ante una autoridad pública independiente para la protección de los derechos asociados al tratamiento de datos personales, principalmente los de acceso y de habeas data.

El capítulo dedicado al régimen de responsabilidad contempla sanciones que van desde la suspensión hasta la clausura de operaciones del banco de datos que

incumpla las normas a las que debe someterse y adiciona un artículo al código penal, que tipifica como punible el tratamiento ilegal de datos.

Se ha incluido un capítulo para el Movimiento Internacional de Datos, donde se fijan las condiciones bajo las cuales es procedente la transferencia internacional de datos. Como regla general, es necesario que el organismo o país destinatario de la información garantice niveles de protección adecuados o similares a los garantizados por la legislación colombiana.

La mencionada ley busca otorgar a las personas una herramienta legal idónea para la protección de sus derechos fundamentales a la intimidad, honra y buen nombre, en relación con el tratamiento de datos de carácter personal que realizan los bancos de datos o centrales de información, derechos que han resultado afectados en numerosas ocasiones debido justamente a la ausencia de normas expresas que sujeten su actividad a unos parámetros mínimos de ecuanimidad, prudencia, proporcionalidad y respeto hacia los titulares de la información.

La ley 221/2007 dispone en su artículo 1° que: "tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en algún banco de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15° de la Constitución Política […]". Sin embargo, a continuación indica, a nuestro criterio con una mala técnica legislativa, que también regulará el derecho a la información, especialmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

Actualmente se debate en Colombia la promulgación de una nueva ley en materia de protección de datos personales. El jueves 6 de octubre de 2011 el Presidente de la Corte Constitucional de la República de Colombia anunció que el Alto Tribunal encontró ajustado a la Constitución la mayoría del texto conciliatorio del proyecto de ley estatutaria Nº 184 de 2010 (Senado) y 046 de 2010 (Cámara)

por la cual se dictan disposiciones generales para la protección de datos personales en Colombia. Unos artículos fueron declarados inexigibles totalmente (27, 29, 30 y 31) y otros inconstitucionales parcialmente (8, 20,23 y 26).

La Corte Constitucional de la República de Colombia que se ocupa de este tema en la Sentencia número C-748 de 2011[391].

9.- Chile

La Constitución Política de la República de Chile[392] (aprobada en 1980 y reformada sustancialmente en 1989 y en 1991), no legisla en forma expresa sobre la protección de datos personales, sólo lo hace indirectamente en los artículos 19.4 y 19.12. Concretamente el art. 19.4 garantiza a toda persona el respeto y protección a su vida privada, a su honra, a la de su familia y a la libertad de información.

El inciso 12° del artículo 19° de la Constitución consagra la libertad de emitir opinión y de informar sin censura previa, sin que pueda interpretarse que la libertad de informar implique la posibilidad de acceder o dar acceso a datos de carácter personal.

En base a los preceptos constitucionales mencionados, la jurisprudencia ha aceptado planteos de acciones judiciales de protección, para proteger los derechos afectados por el tratamiento de datos personales de los accionantes. Muchas de estas acciones fueron resueltas por la Corte Suprema de Justicia chilena.

La ley 19.628[393] sobre Protección de la Vida Privada publicada y vigente a partir del 28 de septiembre de 1999 es una consecuencia directa de la actividad

[391] Corte Constitucional de la República de Colombia: Sentencia número C-748 de 201. Fci: http://www.corteconstitucional.gov.co/comunicados/No.%2040%20comunicado%2005%20de%20octubre%20de%202011.php (último ingreso el 1/2/2012).
[392] La Constitución Política de la República de Chile del año 1980 con las reformas del año 1989. Fci: http://www.georgetown.edu/pdba/Constitutions/Chile/chile89.html.
[393] La ley 16628 (Chile). Sancionada por el Congreso Nacional el 30/8/99, promulgada el 18/9/99 y publicada en el Boletín Oficial el 28/9/99.

judicial desarrollada sobre el tema. Esta norma fue parcialmente modificada en el año 2002 por la ley 19.812[394].

El objeto de la ley es el tratamiento de los datos de carácter personal realizado en registros o bancos de datos, por organismos públicos o por particulares. El artículo 1º exceptúa el tratamiento de datos que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regula por la ley a que desarrolla el artículo 19 inc. 12 de la Constitución Política[395].

El legitimado activo para demandar es el titular de los datos, definido por el art. 2 inciso ñ: como la persona natural a la que se refieren los datos de carácter personal. Este mismo artículo en su inciso f da el concepto de datos personales o datos de carácter personal, diciendo que son los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

La ley 19.628 protege los datos personales de las personas físicas o naturales sin comprender a los datos referidos a personas jurídicas. A nuestro entender, es acertada la reducción del alcance del objeto de la ley, ya que la intimidad de las personas jurídicas puede ser contradictoria en un estado de derecho que exige la transparencia de las personas ideales. La reducción del objeto de la ley a la protección de los datos de las personas físicas, evita amparar a fundaciones, asociaciones civiles y sociedades comerciales que bajo un aparente objeto permitido por la ley, sean instrumento para el fraude, el blanqueo de dinero proveniente de venta de armas, narcotráfico y otros delitos similares, burlando la legislación de sociedades y los controles que debe hacer el Estado a este tipo de organizaciones.

Las personas físicas, titulares de los datos, tienen derecho (art. 12º) a exigir, al responsable del banco de datos, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son

[394] La ley 19.812 (República de Chile) fue publicada en el Boletín Oficial el 13/06/2002.
[395] El artículo 19, inciso 12 consagra las libertades de emitir opinión y de informar sin censura previa en cualquier forma y por cualquier medio.

transmitidos regularmente. En caso que los datos personales sean erróneos o inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen. Sin perjuicio de las excepciones legales, podrá además, exigir que los datos se eliminen, en caso de que su almacenamiento carezca de fundamento legal, o cuando quedare caduco. Igual exigencia de eliminación, o de bloqueo de los datos, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

Las consultas de la información, modificación o eliminación de datos son en principio gratuitas.

El responsable del registro o banco de datos es el legitimado pasivo de la ley. El art. 2º inc. n) determina como responsable del registro o banco de datos a la persona natural o jurídica privada, o al respectivo organismo público, a quien competen las decisiones relacionadas con el tratamiento de los datos de carácter personal.

El mayor defecto de la ley chilena radica en el órgano de control. Ya que mientras el derecho comparado en general (legislación europea, Argentina[396], etc.), crea una autoridad de aplicación y control especial sobre protección de datos personales, la Ley chilena de protección de la vida privada opta por un sistema de control judicial[397] que, en el caso de organismos públicos, es fortalecido por un control cruzado con el Servicio de Registro Civil e identificación de las personas. El artículo 16º expresa que si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al Juez de Letras en lo Civil del

[396] Ley 25326 del año 2000 (Argentina).

[397] En la legislación comparada encontramos diferentes tipos de organismos de control: a) Autoridad independiente, b) Autoridad dependiente del Gobierno, c) No crear ninguna autoridad y que sean los jueces los que ejerzan el control de la aplicación de la Ley (sistema elegido por la ley Chilena) y d) Autoridad dependiente del Parlamento.

domicilio del responsable, solicitando amparo a los derechos consagrados en el artículo 15º. El art. 16º establece las reglas del procedimiento[398].

Con respecto al control de los bancos o archivos de datos, el artículo 22º de la ley determina que el servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos. Este registro tiene carácter de organismo público, responsable del banco de datos que proporciona estos antecedentes al servicio de registro civil e identificación cuando

[398] El art. 16º de la ley chilena 19628 establece en su parte final las reglas del procedimiento para accionar por parte del titular de los datos: a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso. b) El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte. c) El responsable del banco de datos deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada. d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere la letra anterior, sea que se hayan o no presentado descargos. Si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta. e) Todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario. f) La sentencia definitiva será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan. g) Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes. h) El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación. En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente. La sala de la Corte Suprema que conozca la reclamación conforme al inciso anterior, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento establecido en los incisos primero y segundo, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. En las reclamaciones por las causales señaladas en el inciso precedente, el Presidente del Tribunal dispondrá que la audiencia no sea pública. En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales. La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el Tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días.

se inician las actividades de procesamiento de datos personales y comunica cualquier cambio dentro de los quince días desde que se produzca.

En el año 2001, la Corte de Apelaciones de la ciudad de Santiago de Chile rechazó con costas un recurso de protección de garantías constitucionales, en contra de la Corporación Administrativa del Poder Judicial, planteado por una persona que figuraba en el sitio web del Poder Judicial de Chile por haber sido parte en un proceso judicial civil sobre un reclamo de paternidad. El actor demandaba la vulneración del carácter secreto de un proceso de filiación, dado que cualquier persona podía ingresar por internet al sitio web del Poder Judicial y conocer sus datos, el objeto del juicio y la información sobre la persona demandada. Consideró contrarios estos hechos al Código Civil chileno (art. 197) y a la ley 19.628 de Protección de la Vida Privada, antes comentada. Sin embargo, la Corte de Apelaciones de Santiago rechazó el recurso por considerar que no se habían violentado las prescripciones de la ley 19.628 sobre Protección de la vida privada, porque los datos divulgados por el Poder Judicial no eran datos sensibles, porque el Poder Judicial tiene que cumplir con el principio de publicidad de sus actuaciones judiciales y que además no se había vulnerado el carácter de secreto del proceso de filiación, ya que no se habían transcripto las resoluciones del juicio en el sitio web.

10.- Costa Rica

La República de Costa Rica es un país pluricultural de Centroamérica que limita al norte con la República de Nicaragua y al sur con la República de Panamá. Se destaca por ser una de las democracias más consolidadas de América[399].

Aun cuando la Constitución Política de la República de Costa Rica y los diversos tratados internacionales de protección de derechos humanos ratificados por el Estado, contemplan la protección de los derechos y libertades fundamentales, el derecho a la intimidad carece, de un mecanismo ágil y eficiente para su protección.

[399] Puede consultarse la siguiente fci.: http://es.wikipedia.org/wiki/Costa_Rica.

Ciertamente el derecho a la intimidad, a la libertad y al secreto de las comunicaciones se encuentra declarado y garantizado por el artículo 24 de su Constitución, pero aun así huelgan los mecanismos e instrumentos de garantía necesarios para su efectiva protección.

Además podemos mencionar como una norma relacionada por la apertura que realiza al reclamo de otros derechos, al artículo 48 de la Constitución de Costa Rica, dado que al momento de establecer la garantía del *habeas corpus* y el derecho al recurso de amparo expresa que: "Toda persona tiene derecho al recurso de habeas corpus para garantizar su libertad e integridad personales, y al recurso de amparo para mantener el goce de los otros derechos consagrados en esta Constitución [...]".

El art. 28 de la Carta Magna de Costa Rica expresa que todas las acciones privadas que no dañan la moral, o el orden público o a terceros están fuera de la acción de la ley. Esto se refiere al principio de libertad.

El artículo 30 garantiza el derecho al acceso a la información sobre asuntos de interés público, aun cuando excluye a los secretos de Estado. El artículo 33 indica que "Todo hombre es igual ante la ley y no podrá hacerse discriminación alguna contraria a la dignidad humana". El artículo 41 garantiza que "concurriendo a las leyes, todos han de encontrar reparación para las injurias o daños que hayan recibido en su persona, propiedad o intereses morales. Debe hacérseles justicia pronta, cumplida, sin denegación y en estricta conformidad con las leyes".

También podemos citar como un marco jurídico relacionado con la protección de los datos personales a aquellos derechos que otorgan los tratados y demás instrumentos internacionales a los cuales se encuentra adherido el Estado de Costa Rica. Entre ellos podemos mencionar: La Declaración Universal de los Derechos Humanos, que en su artículo 8 indica que "Toda persona tiene derecho a un recurso efectivo, ante los tribunales nacionales, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución o la ley". El artículo 12 del tratado mencionado proclama que "Nadie será objeto de injerencias

arbitrarias en su vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

La Declaración Americana de los Derechos y Deberes del Hombre, en su artículo 5 declara que "Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar".El artículo 18 de esta Declaración expresa que "Toda persona puede recurrir a los tribunales para hacer valer sus derechos. Asimismo, debe disponer de un procedimiento sencillo y breve por el cual la justicia la ampare contra actos de la autoridad que violen, en perjuicio suyo, alguno de los derechos fundamentales consagrados constitucionalmente".

El mencionado artículo 18 de la Declaración Americana de los Derechos y Deberes del Hombre nos da pie para mencionar que dentro de la doctrina del derecho constitucional de nuestro tiempo, se establecen una serie de derechos y libertades básicas para todos los ciudadanos, que requieren para su efectiva protección un mecanismo de garantía o sistema procesal constitucional ágil y rápido, presente en todos los ordenamientos jurídicos. Entre tales derechos y libertades podemos citar, por ejemplo: el derecho a la vida, el derecho a la integridad personal, el derecho a la libertad religiosa e ideológica, el derecho a la libre circulación y los derechos a la intimidad y a la autodeterminación informática, sobre los que se ocupa esta tesis, entreotros.Yase ha mencionado en el capítulo I que, dentro de la esfera del derecho a la vida privada, se encuentran internacionalmente reconocidos el derecho a la intimidad personal y familiar, el derecho al honor, el derecho a la imagen propia y el derecho al secreto de las comunicaciones, todos ellos derechos personalísimos e inalienables, que configuran el círculo más puro de la persona: su fuero interno. Este es el fundamento de su protección.

Aun cuando Costa Rica es reconocida en el mundo por su consolidada democracia y por contar con un aparato institucional y jurídico de avanzada en

materia constitucional, que garantiza una efectiva protección a las personas contra los ataques de terceros a los derechos humanos y civiles, todavía no ha desarrollado un mecanismo jurídico claro y específico para garantizar la protección del derecho a la vida privada y a la autodeterminación informativa de las personas.

En otras palabras, la protección jurídica de los datos de carácter personal o habeas data propiamente dicho, aún no se encuentra contemplada en la Constitución Política de la República de Costa Rica, ni en la legislación del Estado.

Es curioso que en cambio, como ya mencionamos, la Constitución sí regula en el artículo 30[400] el acceso a la información también llamado *habeas data* impropio, instituto por medio del cual se reconoce el derecho de libre acceso a los departamentos administrativos con el propósito de recabar información sobre asuntos de interés público no cubiertos por el secreto de Estado[401].

Volviendo al 24 de la Constitución de Costa Rica, reformado en mayo de 1996, por el cual se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones[402], observamos que pasaron más de quince años desde su incorporación al texto de la Carta Magna, sin que su parlamento lograra acordar un desarrollo legislativo infra constitucional a este precepto.

Por ello, a falta de tutela normativa, entendemos que la protección de los datos de carácter personal puede hacerse efectiva por medio del pronunciamiento jurisprudencial, dado que además de los derechos a la intimidad, a la libertad y al secreto de las comunicaciones contemplado por el artículo 24, la Constitución de la República de Costa Rica ha consagrado los otros principios ya mencionados, tales como el principio de reserva o libertad (art. 28 C.N); los principios de igualdad y no discriminación (art. 33 C.N.); los derechos a la reparación y pronta justicia (art.

[400] El texto de la Constitución Política de Costa Rica, puede ser consultado en el sitio web: http://www.constitution.org/cons/costaric.htm

[401] Artículo 30, Constitución de Costa Rica: **"**Se garantiza el libre acceso a los departamentos administrativos con propósitos de información sobre asuntos de interés público. Quedan a salvo los secretos de Estado".

[402] Reforma Constitucional de 29 de mayo de 1996.

41 C.N.), el derecho al recurso de amparo (Art. 48 de la Constitución) otorgado a toda persona para mantener o restablecer el goce de los otros derechos consagrados en la Constitución; junto a los demás derechos humanos reconocidos en acuerdos y tratados internacionales, aplicables en Costa Rica[403].

También es dable mencionar que la ley Nº 7135 de la jurisdicción constitucional[404], en su artículo 2º, otorga competencia a la jurisdicción constitucional para garantizar, mediante los recursos de *habeas corpus* y de amparo, los derechos y libertades consagrados por la Constitución Política y los derechos humanos reconocidos por el derecho internacional vigente en Costa Rica.

El artículo 57 de la mencionada ley 7135, establece que "el recurso de amparo también se concederá contra las acciones u omisiones de sujetos de derecho privado, cuando estos actúen o deban actuar en ejercicio de funciones o potestades públicas, o, se encuentren, de derecho o de hecho, en una posición de poder frente a la cual los remedios jurisdiccionales comunes resulten claramente insuficientes o tardíos para garantizar los derechos o libertades fundamentales a que se refiere el artículo 2º, inciso a) de la propia ley*"*.

El artículo 66 de la norma *ut supra* mencionada expresa que el recurso de amparo garantiza el derecho de rectificación o respuesta que se deriva de los

---

[403] Entre tales tratados, suele citarse la Declaración Universal de los Derechos Humanos, arts. 8º (derecho a un recurso efectivo, ante los tribunales nacionales, contra actos que violen los derechos fundamentales reconocidos por la Constitución o la ley) y 12 (prohibición de injerencias arbitrarias en la vida privada y familiar, del domicilio y la correspondencia y de ataques a la honra o reputación), y la Declaración Americana de los Derechos y Deberes del Hombre, arts. 5º (derecho a la protección legal contra los ataques abusivos a la honra**,** a la reputación y a la vida privada y familiar) y 18 (derecho a la protección judicial y a disponerse un procedimiento judicial sencillo y breve en amparo contra actos de autoridad que violen alguno de los derechos fundamentales consagrados constitucionalmente).

[404] Ley N° 7135, del 19 de octubre de 1989, que regula los principales aspectos del sistema costarricense de justicia constitucional concentrada -es de competencia exclusiva de la sala constitucional el conocimiento de la acción de inconstitucionalidad, del amparo, tanto contra los poderes públicos como contra los particulares, de los conflictos de competencia, del *habeas corpus* y de las consultas de constitucionalidad ya sean judiciales o legislativas-, norma considerada en su momento como una verdadera revolución jurídica, pues permitió poner en práctica y funcionamiento el contenido de las normas constitucionales para darles una debida aplicación, pero que trajo como consecuencia "la saturación de asuntos en la sala" (Fallas Vega, Elena.*Informe Jurídico).*

artículos 29 de la Constitución Política y 14 de la Convención Americana sobre Derechos Humanos, a toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio, por medios de difusión que se dirijan al público en general, y, consecuentemente, para efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establece la misma ley; y que en ningún caso la rectificación o la respuesta eximirá de otras responsabilidades legales en que se hubiese incurrido.

Del cuadro normativo esbozado, se observa, entonces, que aun cuando la Constitución Política de Costa Rica no contiene una garantía específicamente diseñada para la tutela de los datos de carácter personal que pudieran verse vulnerados a partir de un tratamiento automatizado, el habeas data si puede ser planteado y resuelto por la jurisprudencia, dado que por imperio del principio de razonabilidad, la protección de datos personales y la autodeterminación informativa, en tanto derechos fundamentales de toda persona, así considerados pacíficamente por la doctrina internacional, deben ser protegidos aun cuando se encuentre ausente la mención expresa en la norma constitucional y su desarrollo en una norma infra constitucional que reglamente el ejercicio de las acciones para su protección.

De hecho, los avances que se lograron en Costa Rica, en esta materia, llegaron de la mano de la interpretación jurisprudencial constitucional. La Sala Constitucional ha reconocido al *habeas data* como un derecho fundamental y autónomo, encuadrado dentro de los derechos implícitos, o no enumerados por la Constitución[405]. Esta jurisprudencia ha fundamentado la protección del derecho a la protección de los datos personales por medio del otorgamiento del *habeas data*, como una derivación del art. 24 de la Constitución Política de Costa Rica, y tiene expresado que el derecho a la autodeterminación informativa es una ampliación del derecho a la intimidad.

[405] Basterra, M. (2008). Op. Cit.; p. 229.

En la Sentencia N° 8996-2002, la Sala Constitucional de la Corte Suprema de Justicia Costa Rica[406] ha establecido que el *habeas data* para los tribunales de justicia de Costa Rica incluye los derechos al acceso, a la actualización, a la rectificación, a la confidencialidad, a la exclusión, a la inserción y a saber del conocimiento de terceros sobre la información recolectada. Esta Sentencia también sirvió para que la Sala Constitucional estableciera los principios generales que debe tener un sistema de protección de datos personales.

Aun cuando es destacable el trabajo de los tribunales de Costa Rica en materia de protección de datos personales, es necesaria la promulgación de una ley reglamentaria que regule el proceso de *habeas data*. Sin embargo, por la naturaleza evolutiva del derecho y por la acción de sus operadores (la jurisprudencia es una prueba de ello) la expresa regulación del *habeas corpus* y del amparo indican la necesaria y pronta incorporación del instituto del *habeas data* dentro del plexo constitucional de Costa Rica.

Entre los antecedentes del tema encontramos que en la Asamblea Legislativa de Costa Rica se presentó en el año 1996 un proyecto de ley[407], de autoría del Diputado Constantino Urcuyo Fournier sobre el recurso de *habeas data*, titulado: "Adición de un nuevo capítulo IV, denominado del Recurso de Habeas Data, al título III de la Ley de Jurisdicción Constitucional, Ley Nº 7135[408]". La exposición de motivos del mencionado proyecto, presenta un análisis de los alcances y ventajas de contar con la figura del recurso de *habeas data* en la legislación de Costa Rica. El proyecto mencionado fue analizado por la Comisión Permanente de Asuntos Jurídicos, la cual, luego de realizar una serie de consultas a diversas instituciones, dio un dictamen afirmativo, que no corrió igual suerte en la Sala Constitucional, donde recibió algunas observaciones, y finalmente fue archivado.

---

[406] Corte Suprema de Justicia de Costa Rica: Sala Constitucional.
Fci: http://www.poder-judicial.go.cr/salaconstitucional/.

[407] El sitio web de la Asamblea Legislativa de la República de Costa Rica, es el siguiente: www.racsa.co.cr/asamblea.

[408] Proyecto de ley tramitado en el Expediente Nº 17785 de la Asamblea Legislativa de Costa Rica.
Fci: http://www.racsa.co.cr/asamblea/proyecto/tx_base/14785.doc.

Posteriormente ingresó a la Asamblea Legislativa un nuevo proyecto de ley sobre *habeas data* y protección de datos personales, presentado por el Diputado Rolando Laclé Castro, el 18 de junio de 2002 (Expediente Nº 14.745), que cuenta con idéntico título y contenido que el proyecto antes mencionado. Esta nueva iniciativa parlamentaria busca retomar y proponer como base de discusión el dictamen de la Comisión Permanente de Asuntos Jurídicos del viejo proyecto de Urcuyo Fournier.

En concreto, el proyecto de ley propone adicionar a la ley de la Jurisdicción Constitucional un nuevo recurso que regule dos tipos de *habeas data*: el propio y el impropio[409]. El *habeas data* propio, previsto en el artículo 71[410], tutela la información personal, y el *habeas data* impropio garantiza el acceso a la información pública, en el art. 72[411] del proyecto de ley.

El *habeas data* propiamente dicho del proyecto de ley debatido en Costa Rica otorga legitimación activa a toda persona física o jurídica para conocer lo que

[409] Puccinelli, O. (1999). Op. cit., p. 521.

[410] Artículo 71 del Proyecto de Ley Nº 14.745: El recurso de habeas data tiene por objeto proteger de manera procedimental el derecho de la persona a su intimidad, imagen, honor, autodeterminación informativa y libertad informática en el tratamiento de sus datos personales. Asimismo, es objeto de este recurso garantizar el ejercicio pleno de todos los derechos y las libertades concernientes a los datos y la información de carácter personal.

[411] Artículo 72 del Proyecto de Ley Nº 14.745: El recurso de habeas data podrá plantearse en los siguientes casos: a) Toda persona, física o jurídica, podrá plantearlo para conocer lo que conste sobre sí misma o sus bienes en registros, archivos, listados o bancos de datos, sean manuales, mecánicos, electrónicos o informatizados, públicos o privados. No podrán solicitarse datos sobre una investigación judicial por la comisión de algún delito, mientras no haya concluido el proceso investigador. b) La pretensión del recurso de habeas data puede consistir en solicitar información sobre la finalidad de los datos personales recogidos, su destino final y su eventual entrega en otros lugares de procesamiento de datos distintos del lugar que, en primera instancia, recolectó los datos. c) Mediante el recurso de habeas data podrá requerirse la rectificación, actualización, inclusión, confidencialidad o cancelación inmediata de los datos personales que están en poder del lugar de tratamiento de los datos, ya sea público o privado. d) El recurso de habeas data también procederá para solicitar informaciones declaradas secreto de Estado. La Sala en pleno deberá determinar si tales informaciones se ajustan a los requerimientos constitucionales. Para los efectos de esta norma, secretos de Estado son los asuntos en tramitación, de carácter diplomático o referido a operaciones de seguridad nacional pendientes. e) Podrá plantearse el recurso de habeas data cuando se haya lesionado alguno de los principios relacionados con el procesamiento de datos personales descritos en el artículo 73. f) El afectado podrá impugnar, mediante la presentación del recurso de habeas data, los actos administrativos o las decisiones de carácter particular que impliquen una valoración de su comportamiento, cuya única base sea un tratamiento de datos personales que defina sus características o personalidad.

conste sobre sí misma o sobre sus bienes, así como la finalidad a que se destine esta información. Se trata del derecho de acceso a los registros de información personal para tomar conocimiento de los datos propios y su finalidad, para eventualmente requerir su rectificación, actualización, inclusión, confidencialidad o cancelación inmediata.

El *habeas data* impropio proyectado en esta iniciativa legislativa garantiza el derecho a solicitar información pública, no personal del peticionario contenida en registros, listados, archivos o bancos de datos, siempre y cuando el sujeto demuestre que tiene un interés legítimo para acceder a esos datos. Establece cierto control judicial sobre la declaración de secreto de Estado sobre este tipo de información.

El proyecto de ley propone, para la acción de *habeas data*, el trámite del amparo[412], el cual debe resolverse con prioridad a otros recursos de amparo y emplaza al juez para que el dictado de la sentencia no demore más de cinco días naturales después de recibidas las pruebas del caso.

La legitimación activa para interponer el recurso de habeas data está reglada en el artículo 75 del proyecto[413], el cual otorga legitimación activa a las personas físicas; a los herederos del difunto, ascendientes y descendientes, colaterales hasta el cuarto grado y al cónyuge; a las personas jurídicas, al defensor de los habitantes y a las asociaciones representativas de habitantes, por actos de discriminación.

Como sujeto pasivo del habeas data propio, contemplado en el art. 71 del proyecto, incluye en forma amplia, a los registros, archivos, listados o bancos de datos, sean manuales, mecánicos, electrónicos o informatizados, públicos o privados.

[412] Artículo 74. El recurso de habeas data recibirá el trámite establecido para el amparo. Se resolverá con prioridad respecto a otros recursos de amparo, salvo los fundamentados en el derecho de rectificación y respuesta y el de petición. Deberá dictarse sentencia a más tardar cinco días naturales después de recibidas las pruebas del caso.

[413] Artículo 75. El recurso podrá ser interpuesto por: a) La persona física o su representante, en el caso de menores de edad o incapaces. b) Los herederos del difunto. c) Las personas jurídicas.

El art. 72 del proyecto determina como eventual sujeto pasivo a los registros, listados, archivos o bancos de datos en el *habeas data* impropio. La falta de precisión del art. 72 no aclaraba si permitía el acceso a la información pública contenida en archivos privados o si únicamente daba legitimidad pasiva a los archivos públicos.

La mayor crítica que podemos hacer a este proyecto, es que no crea una autoridad de aplicación y control para la protección de los datos de carácter personal, sin la cual, en caso de ser promulgado como ley, puede nacer como una norma débil y agonizante.

11.- Ecuador

La República de Ecuador incorporó en su reforma constitucional del año 1996, el artículo 30, dentro del cual expresa que: *"*toda persona tiene derecho a acceder a la documentación, bancos de datos e informes que sobre sí misma o sobre sus bienes consten en entidades públicas o privadas, así como conocer el uso que se haga de ellos y su finalidad. Igualmente podrá solicitar ante el funcionario o juez competente la actualización, rectificación, eliminación o anulación de aquellos, si fueren erróneos o afectaren ilegítimamente sus derechos. Se exceptúan los documentos reservados por razones de seguridad nacional*"*. Aquí encontramos el primer antecedente constitucional del *habeas data* en Ecuador, aun cuando esta norma no menciona expresamente al instituto del *habeas data*, ni contempla sus diferentes tipos.

Posteriormente, la Constitución de la República de Ecuador[414], aprobada el 11 de agosto de 1998[415], ha incluido el recurso de *habeas data* como una garantía

[414] *Constitución Política de la República del Ecuador*. Editorial EDIJUR, Quito (Ecuador); 2003, p.38. Esta fuente también puede consultada Internet.
Fci: http://www.georgetown.edu/pdba/Constitutions/Ecuador/ecuador98.htmt.
[415] La Constitución de 1998 derogó la Constitución de 1996, la cual legisló sobre el habeas data en el artículo 30. La consulta de la Constitución Política de Ecuador de 1996 puede hacerse en el sitio web: www.georgetown.edu/pdba/Constitutions/Ecuador/ecuador96.html.

constitucional expresa, ubicada dentro de la Sección referida a las Garantías de los Derechos.

El artículo 94º otorga a toda persona el derecho a acceder a los documentos, bancos de datos e informes que sobre si misma o sobre sus bienes, consten en entidades públicas o privadas, así como para conocer el uso y el propósito que se haga de ellos. Las personas también pueden solicitar, ante el funcionario respectivo, la actualización de los datos, su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. El afectado puede demandar una indemnización, si la falta de atención le causare algún perjuicio.

El acceso a los datos personales que consten en los archivos vinculados con la defensa nacional, requiere un procedimiento especial que debe ser establecido por ley del Congreso[416].

La acción de *habeas data* tiene por objeto: a) El acceso a los documentos, bancos de datos e informes sobre el afectado o sobre sus bienes obrantes en entidades públicas o privadas; b) La información sobre el uso que de ellos se haga y la finalidad para la cual se los tiene registrados, y c) La petición de actualización, rectificación, eliminación o anulación de los datos que fueren erróneos o afectaren ilegítimamente sus derechos, ante el funcionario o juez competente.

El cuadro normativo de la protección de datos personales se completa en Ecuador con la Ley del Control Constitucional[417] promulgada en 1997. Esta ley entró en vigencia un año después de sancionada la constitución de 1996, que ya legislaba sobre el habeas data en el título II dedicado a las garantías de los derechos de las personas[418].

---

[416] *Constitución Política de la República del Ecuador. Ley de Control Constitucional*. Editorial Galbar, Quito (Ecuador), 2002, p. 38.
[417] Publicada en el Reg. Oficial Nº 99 del 2 de julio de 1997.
[418] Falconi, J. *El Juicio Especial por la acción de habeas data; y los derechos constitucionales a: la intimidad; privacidad; imagen; al honor; a la no discriminación; a la igualdad; al de petición; al de información, sus limitaciones y responsabilidades*. Editorial Rodin. Quito (Ecuador), 2000, p. 16.

El artículo 94º de la Constitución establece, en términos amplios, que toda persona tiene derecho a acceder a los documentos, bancos de datos e informes que sobre ella, o sobre sus bienes consten en entidades públicas o privadas

De manera concordante con la extensión del derecho de acceso otorgado a todas las personas, la Ley de Control Constitucional habilita a interponer el recurso de *habeas data* (art. 34), a las personas naturales o jurídicas, nacionales o extranjeras, que deseen tener acceso a documentos, bancos de datos e informes que sobre sí mismas o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les esté por dar. El recurso permite requerir las respuestas ante quienes posean tales datos o informaciones y exigirles el cumplimiento de medidas tutelares prescritas en la ley.

En lo relativo al sujeto pasivo, la Constitución establece que toda persona tiene derecho a interponer *habeas data* respecto de documentos, bancos de datos e informes que consten en "entidades públicas o privadas", sin distinciones.

En consonancia con ello, la ley de control constitucional establece que *el habeas data* puede ser dirigido contra entidades públicas, personas naturales o jurídicas privadas que posean tales datos o informaciones (art. 34), aunque luego, en su artículo 36, menciona algunas de las limitaciones que tradicionalmente se hacen a su ejercicio, por cuestiones no vinculadas a la calidad de la persona hacia la cual va dirigida, sino por la actividad que esta despliega (cuando se afecte al sigilo profesional; cuando los documentos que se soliciten tengan el carácter de reservados por razones de seguridad nacional, o cuando por disposición de la ley deban mantenerse registrados).

El art. 35 de la Ley de Control Constitucional indica que el recurso de *habeas data*tiene por objeto: a) Obtener del poseedor de la información que este la proporcione al recurrente, en forma completa, clara y verídica. b) Obtener el acceso directo a la información. c) Obtener de la persona que posee la información que la

rectifique, elimine o no la divulgue a terceros; y d) Obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado o no la ha divulgado.

La ley del control constitucional dispone que el juez ordenará la eliminación, rectificación o reserva, salvo cuando claramente se establezca que la información no puede afectar el honor, la buena reputación, la intimidad o irrogar daño moral al solicitante.

El artículo 36 amplia las excepciones previstas en el texto constitucional, disponer que no es aplicable *el habeas data* cuando afecte el sigilo profesional; o cuando pueda obstruir la acción de la justicia; o cuando los documentos que se soliciten tengan el carácter de reservados por razones de seguridad nacional, y no podrá solicitarse la eliminación de datos o informaciones cuando por disposición de la ley deben mantenerse en archivo o registros públicos o privados.

Cualquier juez o tribunal de primera instancia del domicilio del poseedor de la información o de los datos requeridos es competente para entender en la acción de habeas data.

Planteado el recurso de habeas data, la ley ordena intervención inmediata de los jueces y tribunales competentes, e incluso precisa que en el día hábil siguiente al de la presentación de la demanda, el juez o tribunal competente convocará a las partes a audiencia, que se realizará dentro del plazo de ocho días. Y ordena que la respectiva resolución sea dictada en el término máximo de dos días posteriores a la fecha en que tuvo lugar la audiencia (art. 38º LCC).

Si el Juez o Tribunal Competente hace lugar al recurso, las entidades o personas requeridas deben entregar en el plazo de ocho días y bajo juramento, toda la información y una explicación detallada que incluya: a) Las razones y fundamentos legales que amparen la información recopilada; b) La fecha desde la cual tienen esa información; c) El uso dado y el que se pretenderá dar a ella; d) Las personas o entidades a quienes se les haya suministrado los referidos datos, la fecha

de suministro y las razones para hacerlo; e) El tipo de tecnología que se utiliza para almacenar la información; y f) Las medidas de seguridad aplicadas para precautelar dicha información.

Si el accionante considera insuficiente la respuesta dada por el demandado, puede solicitar que juez disponga la verificación directa, para la cual se facilitará el acceso del interesado a las fuentes de información, proveyéndole el asesoramiento de peritos si así se solicitara.

Si de la información obtenida el interesado considera que uno o más datos deben ser eliminados, rectificados, o no darse a conocer a terceros (art. 41º), puede pedir al juez que ordene al poseedor de la información que así proceda. El juez ordenará tales medidas, salvo cuando claramente se establezca que la información no puede afectar el honor, la buena reputación, la intimidad o irrogar daño moral al solicitante. El depositario de la información debe jurar que dará estricto cumplimiento a lo ordenado por el juez. Previa autorización judicial, el interesado puede verificar el cumplimiento de la orden judicial, solo o acompañado de peritos.

La denegación del recurso de *habeas data* es apelable ante el Tribunal Constitucional, en el término de ocho días apartar de la notificación de la misma.

La legitimación activa para iniciar y continuar los procedimientos correspondientes a la acción de habeas data, recae no solo en las personas naturales o jurídicas que consideren tener derecho a ello, sino también en los padres, tutores y curadores en nombre de sus representados (art. 45º).

Las disposiciones finales del capítulo II de la ley del control constitucional, aplican sanciones contra las personas indicadas como sujetos pasivos del *habeas data*que violen sus disposiciones[419], a saber:

> a) Los representantes legales de las personas jurídicas de derecho privado o las naturales que incumplieren las resoluciones expedidas por

[419] Puccinelli, O. (1999). Op. cit., p. 547.

jueces o tribunales que concedan el *habeas data,* no podrán ejercer ni directa ni indirectamente, las actividades que venían desarrollando y que dieron lugar al *habeas data,* por el lapso de un año, lo cual será comunicado a los órganos de control y demás entidades públicas y privadas que sean del caso (art. 42);

b) Los funcionarios públicos de libre remoción que se nieguen a cumplir con las resoluciones que expidan los jueces o tribunales en el procedimiento del *habeas data* serán destituidos inmediatamente de su cargo o empleo, sin más trámite, por el respectivo juez o tribunal, salvo cuando se trate de los funcionarios elegidos por el Congreso Nacional, quienes deberán ser destituidos por este, a pedido fundamentado del juez o tribunal y previo el correspondiente juicio político; esta sanción se comunicará inmediatamente a la Contraloría General de Estado y a la autoridad nominadora correspondiente (art. 43);

c) Las sanciones antes señaladas se impondrán sin perjuicio de las respectivas responsabilidades civiles y penales a que hubiere lugar (art. 44).

El *habeas data* impropio está destinado a la obtención de información pública. Se encuentra desarrollado en la Ley de Modernización del Estado, que prescribe el derecho de acceso a documentos administrativos del sector público, con el fin de asegurar la actuación administrativa imparcial y correcta.

Lo más criticable de este sistema legal de protección de datos personales, es que la legislación ecuatoriana no ha creado una autoridad de aplicación y control en materia de protección de datos personales.

La jurisprudencia del Tribunal Constitucional de la República de Ecuador, hoy denominada Corte Constitucional[420] por la reforma de la Constitución de 2008,

[420] Corte Constitucional de Ecuador; fci.: http://webtest.corteconstitucional.gob.ec/.

atendió un caso de *habeas data* en el año 2005[421], planteado defectuosamente en contra del Alcalde y del Procurador Síndico de la ciudad de Quito, puesto que el actor al solicitar documentos públicos de la Municipalidad, confundió una acción de acceso a la información pública con una de *habeas data*, ya que el objeto de la demanda no planteaba la protección, acceso, rectificación, cancelación o actualización de sus datos personales. El Tribunal Constitucional de Ecuador, con buen criterio, rechazó este planteo.

12.- México

En el año 2002, entra en vigencia en México la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y se crea el organismo supervisor de dicha ley: el Instituto Federal de Acceso a la Información y Protección de Datos. Su campo de vigilancia, en un comienzo sólo alcanzó a la Administración Pública Federal y a los organismos autónomos como el Instituto Federal Electoral (IFE), la Comisión Nacional de Derechos Humanos (CNDH) y el Banco de México.

En julio de 2007 se implementaron acciones con miras a consolidar la protección de datos personales en posesión de las empresas particulares, pero tuvieron que transcurrir tres años más, y tres modificaciones a artículos de la Constitución Mexicana (6°, 16° y 73°), junto con la transformación del Instituto Federal de Acceso a la Información y Protección de Datos[422](IFAI) para quedar como un organismo público descentralizado de la Administración Pública Federal con autonomía operativa, presupuestaria y de decisión, para recién llegar a la promulgación y posterior publicación, el 5 de julio de 2010, del decreto que expide

[421] Corte Constitucional de Ecuador. Sentencia de fecha 23/03/2005. Fci: http://www.tribunalconstitucional.gov.ec.

[422] Instituto Federal de Acceso a la Información y Protección de Datos (IFAI). Fci.: http://www.ifai.org.mx/

la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)[423].

La LFPDPPP es de orden público y observancia general en toda la República y su objeto es la protección de los datos personales en posesión de particulares para regular su tratamiento legítimo, informado y controlado a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Basada principalmente en el modelo europeo, esta ley se compone de 69 artículos, agrupados en 11 capítulos, que cubren los siguientes temas:

a) Los derechos que otorga la ley, llamados en Méjico derechos ARCO, por medio de los cuales se otorgan las garantías y procedimientos para que cualquier persona pueda acceder, ratificar, corregir y/u oponerse a la existencia de registros con información sensible o no sensible.

b) El derecho al aviso de privacidad, conforme al cual la obtención de datos debe hacerse a través de medios lícitos y no fraudulentos. En el caso de que la información recabada sean datos sensibles, el responsable del banco de datos debe contar con el consentimiento expreso y por escrito del titular de los datos con firma autógrafa; en caso de que no existan datos sensibles bastará una autorización por cualquier medio impreso o electrónico. Además, el aviso de privacidad debe especificar la finalidad de la recopilación de los datos, identidad y domicilio de quien recaba, potenciales transferencias de los datos a terceros (empresas de *outsourcing* o del mismo grupo, nacionales o extranjeras).

c) Tratamiento de datos. El tratamiento de los datos requiere la autorización del titular de los mismos (aviso de privacidad) y éstos sólo se podrán usar para el fin para el cual fueron recabados. El tratamiento de los datos deberá contemplar su protección contra daño, pérdida, alteración, destrucción, acceso o uso no autorizado. Así también el responsable directo

[423] Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Fci.: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

del tratamiento de los datos, o terceros que intervengan en cualquier fase, deberá guardar confidencialidad respecto de éstos aun después de finalizar relaciones con el titular o responsable inscrito en el aviso de privacidad.

d) No cumplimiento. La verificación del cumplimiento de la LFPDPPP queda a cargo del IFAI, y puede iniciarse de oficio o a petición de parte. Cualquier vulneración de la seguridad que afecte los derechos patrimoniales o morales de una(s) persona(s) deberá ser informada inmediatamente al (los) titular(es) de los datos. El no cumplimiento de la ley puede generar infracciones económicas o sanciones penales. Las multas varían desde los valores cercanos a los 500 dólares, hasta llegar al millón y medio de dólares estadounidenses. Las penas por delito pueden ir desde los tres meses hasta los cinco años de prisión, y en el caso de que en el incumplimiento de la ley estén involucrados datos "sensibles" ambas sanciones se duplicarán.

e) Debido a la legislación mexicana y a los artículos transitorios de la ley es importante tener presentes las siguientes consideraciones: El derecho ARCO se podrá ejercer a los dieciocho meses de la entrada en vigor de la ley, esto es a partir del 6 de enero de 2012.

f) Los avisos de privacidad se podrán expedir a más tardar un año después de la entrada en vigor de la ley, esto es, como máximo, el 6 de julio de 2011.

g) El reglamento de la ley se expedirá dentro de los siguientes doce meses a su entrada en vigor, esto es, antes del 6 de julio de 2011.

El IFAI hoy en día se enfrenta a amparos y confrontaciones con organismos de gran relevancia nacional, que incluso pueden llegar a la corte. Respecto a los temas económicos, el IFAI desde 2004 hasta 2010 ha tenido solo el incremento de 1% de su presupuesto en todo ese lapso; en ese mismo periodo las peticiones al instituto crecieron 576%, verificando el cumplimiento de 98% de las resoluciones.

En estos momentos el desafío que se presenta a la protección de datos personales en México, a su legislación regulatoria y al IFAI (Instituto Federal de Acceso a la Información y Protección de Datos) se encuentra en la posibilidad de contar con los recursos presupuestarios y humanos con los cuales realizar la difusión y promoción de estos nuevos derechos, para que las personas los conozcan y comiencen a ejercerlos.

Hasta el año 2005 los Estados Unidos Mexicanos sólo habían legislado sobre la protección de datos personales en forma sectorial, regulando la constitución y operación de las empresas de información sobre riesgo de crédito, por medio de una Ley de orden público y de observancia general en todo su territorio, cuya publicación fue realizada en el Diario Oficial de la Federación el 15 de enero de 2002 con el título de Ley para Regular las Sociedades de Información Crediticia[424].

Esta ley establece en su artículo quinto, que la prestación de servicios consistentes en la recopilación, manejo y entrega o envío de información relativa al historial crediticio de personas físicas y morales, así como a operaciones crediticias y otras de naturaleza análoga que éstas mantengan con Entidades Financieras y Empresas Comerciales, solo podrá llevarse a cabo por Sociedades que obtengan autorización del Estado.

La ley no considera que exista violación al Secreto Financiero cuando sean los usuarios quienes proporcionen información sobre operaciones crediticias u otras de naturaleza análoga a las Sociedades, así como cuando éstas compartan entre sí información contenida en sus bases de datos o proporcionen dicha información a la Comisión. Tampoco considera que existe violación al Secreto Financiero cuando las Sociedades proporcionen dicha información a sus Usuarios, o cuando sea solicitada por autoridad competente, en el marco de sus atribuciones.

[424] Ley Para Regular las Sociedades de Información Crediticia (México), publicada en el Diario Oficial de la Federación el 15 de enero de 2002.
Fci: http://www.shcp.gob.mx/servs/normativ/leyes/l_rsic.html.

Las sociedades de información crediticia solo pueden llevar a cabo las actividades necesarias para la realización de su objeto, incluyendo el servicio de calificación de créditos o de riesgos, así como las análogas y conexas que autorice la Secretaría, oyendo la opinión del Banco de México y de la Comisión Nacional Bancaria y de Valores[425].

La norma bajo examen establece, en su artículo 17, que estas sociedades de información crediticia estarán sujetas a la inspección y vigilancia de la Comisión Nacional Bancaria y de Valores, y deberán proporcionar la información y documentos que el Banco de México determine. También deben presentar (art. 37), a la Comisión, manuales que establezcan las medidas mínimas de seguridad que incluirán el transporte de la información, así como la seguridad física, logística y en las comunicaciones. Estos manuales deben contener, en su caso, las medidas necesarias para la seguridad del procesamiento externo de datos. Los usuarios pueden verificar, con el consentimiento de las Sociedades, que existan las medidas de seguridad necesarias para salvaguardar la información.

La ley les ha prohibido a las sociedades de información crediticia: I. Solicitar y otorgar información distinta a la autorizada conforme a esta ley y a las demás disposiciones aplicables; II. Explotar por su cuenta o de terceros, establecimientos mercantiles o industriales o fincas rústicas y, en general, invertir en sociedades de cualquier clase distintas a las señaladas en la presente ley; y III. Realizar actividades no contempladas en esta ley y demás disposiciones aplicables.

La regulación legal, que estudiamos, permite que solo las entidades financieras y las empresas comerciales puedan ser usuarios de la información que proporcionen las Sociedades de información crediticia. La ley entiende por usuario (artículo 1º), en singular o plural, a las Entidades Financieras oa las Empresas Comerciales que proporcionen información o realicen consultas a la Sociedad.

[425] Artículo 13 de la Ley para la Regulación de las Sociedades de Información Crediticia.

Las personas son denominadas clientes por la ley de regulación de sociedades crediticias. En efecto, el artículo 1º de la Ley en estudio, expresa que, a los efectos de la ley, se entiende por cliente, en singular o plural, a cualquier persona física o moral que solicite o sobre la cual se solicite información a una Sociedad.

Además de multas y sanciones, el artículo 51, incluido dentro del capítulo de las sanciones, determina que las Sociedades responderán por los daños que causen a los Clientes al proporcionar información cuando exista culpa grave, dolo o mala fe en el manejo de la base de datos. Los Usuarios que proporcionen información a las Sociedades igualmente responden por los daños que causen al proporcionar dicha información, cuando exista culpa grave, dolo o mala fe.

En esta ley se percibe una fuerte influencia del sistema judicial de los EEUU, dado que no legisla en forma general la protección de datos personales, ni crea una autoridad de control independiente y autónoma que proteja a las personas de la acumulación indebida de sus datos personales. Además, cabe observar que solo se ha regulado a las sociedades de información crediticia y se ha dejado un gran vacío legal sobre otras bases de datos no relacionadas con la información sobre los riesgos de crédito a una persona. Por este motivo, entendemos que México necesita dar una mayor protección a los datos de las personas que habitan su territorio, ya sea por la vía de una legislación general, tipo ómnibus, o bien por medio de una legislación sectorial, del tipo de la Ley para la Regulación de las Sociedades de Información Crediticia, que alcance a todo otro tipo de bases de datos personales.

Finalmente México promulgó una legislación general sobre protección de datos personales a la que dio por nombre Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), publicada el 05 de julio de 2010, dicha ley está alineada con los preceptos originales que otras naciones, principalmente europeas, imprimieron en sus respectivas leyes de protección de datos: el respeto a los derechos humanos y a las libertades individuales. Veamos en retrospectiva lo que se ha hecho en el mundo para situar en su justa dimensión los esfuerzos de México en relación a este tema.

13.-Paraguay

La Constitución de la República de Paraguay introdujo la protección de los datos de carácter personal con la reforma constitucional del año 1992, en el capítulo de las garantías constitucionales, al receptar el recurso de *habeas data* en el artículo 135.

Este recurso fue calificado por la jurisprudencia como una garantía constitucional tendiente a tornar efectivas algunas previsiones constitucionales, tales como el derecho a la intimidad, la inviolabilidad del patrimonio documental y la comunicación privada o la protección de la dignidad y de la imagen privada de las personas.

La Constitución define como sujeto activo del recurso de habeas data a toda persona, expresión entendida tanto por la jurisprudencia como por la doctrina, con alcance a todas las personas tanto físicas como jurídicas. De esta forma el constituyente dejó la suficiente amplitud como para contrarrestar cualquier tipo de limitación arbitraria que el Poder Ejecutivo pudiera intentar hacer por vía de reglamentación, pero no realizó mención expresa que permita la posibilidad de extender la legitimación activa a los familiares en defensa de la intimidad familiar, o al defensor del pueblo, como ocurre en otras normas del derecho comparado.

Entonces, el recurso de habeas data otorga a toda persona los siguientes derechos: a) a acceder a la información que sobre la persona del accionante, o sobre sus bienes, obren en registros oficiales o privados de carácter público; b) a conocer el uso que se haga de los mismos y su finalidad; y c) a solicitar, ante el magistrado competente, si los datos fuesen erróneos o afectaren ilegítimamente los derechos del afectado: la actualización, la rectificación, o la destrucción de los mismos.

Puede observarse que la Constitución, además de garantizar el acceso a la información personal, su uso y finalidad, también otorga al sujeto activo las facultades para hacer actualizar, rectificar o destruir la información que sea errónea, o que afecte ilegítimamente sus derechos.

Los sujetos pasivos del recurso de *habeas data* son todos los registros oficiales o privados de carácter público que contengan información del sujeto

activo. Algunos autores han criticado que el texto constitucional se limite únicamente a los archivos que tuvieran carácter público, y por el contrario, entienden que el recurso de habeas data debería alcanzar también a los archivos privados, que no tuvieren carácter público. Sin embargo, el constituyente paraguayo excluyó del recurso de habeas data el acceso a los archivos de carácter privado para no vulnerar la disposición constitucional que garantiza la inviolabilidad de los papeles privados.

Del texto constitucional, por ejemplo, surge en forma tácita que la Policía está pasivamente legitimada para responder ante un recurso de habeas data por los datos personales que mantiene en su poder, ya que sus archivos no son registraciones privadas. La Constitución atribuye el carácter de sujeto pasivo del recurso de habeas data a los registros oficiales o privados de carácter público. La frase no contempla todos los supuestos posibles, pero permite que la reglamentación se adapte a los objetivos que puede perseguir el afectado y a la interpretación del caso concreto.

La protección de los datos personales, que realiza el recurso de *habeas data* en el artículo 135 de la Constitución paraguaya, no debe confundirse con el, denominado por algunos autores *habeas data* impropio, ubicado en los artículos 26 y 28 de la Carta Magna, ya que estos preceptos constitucionales sólo tienen por objeto garantizar el acceso a la información pública.

La Constitución también ordenó la reglamentación del recurso de habeas data por medio de una ley, en forma expresa. El parlamento paraguayo demoró ocho años en cumplir con el mandato constitucional y sancionar la ley 1682 de diciembre del año 2000.

La ley 1682/2001[426] desarrolló la norma constitucional y reglamentó en escuetos 11 artículos, el uso de la información de carácter privado. En su artículo 1º, la ley expresa que "Toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado".

---

[426] Fci: http://www.redipd.org/documentacion/legislacion/common/legislacion/paraguay/Ley_1682_de_2001.pdf

Define a los datos sensibles en su artículo 4º, como los datos referentes a pertenencias raciales o étnicas, preferencias políticas, estado individual de salud, convicciones religiosas, filosóficas o morales; intimidad sexual y, en general, los que fomenten prejuicios y discriminaciones, o afecten la dignidad, la privacidad, la intimidad doméstica y la imagen privada de personas o familias. La ley prohíbe dar a publicidad o difundir datos sensibles, cuando pertenezcan a personas que sean explícitamente individualizadas o individualizables.

El punto más criticable de la legislación paraguaya de protección de datos personales es la ausencia de una autoridad de aplicación y control en la materia. Por el contrario, ha dejado estas competencias en manos del Juzgado en lo Civil y Comercial, en trámite sumario, es decir que se ha pronunciado a favor del sistema del control judicial de la aplicación de la ley 1682 y toda otra normativa referida a la protección de datos personales. No consideramos correcta esta opción, puesto que además de recargar el trabajo judicial de juzgados, muchas veces ya saturados de trámites y procesos, obliga al titular del dato a judicializar una cuestión que muchas veces podría solucionarse con un trámite o denuncia administrativa ante un organismo de control especializado. Tengamos en cuenta que la tramitación judicial es generalmente lenta y que requiere la representación de un abogado con el encarecimiento del costo de la reclamación que eso implica. Nos parece más acertado el modelo legislativo europeo, seguido por Méjico y Argentina, entre otros, en el cual se crea una autoridad de aplicación especializada con el fin de velar por el cumplimiento de la ley y por la protección de las personas en este derecho fundamental. Otro debate ya profundizado en el capítulo I de estos estudios, es la capacidad, independencia, autonomía y presupuesto con el que hay que dotar a estos organismos para su funcionamiento eficaz.

14.- Uruguay

Uruguay es el único país del Mercosur que no ha incluido en su Constitución el recurso garantía de habeas data para proteger jurídicamente los datos personales de las personas que habitan su territorio nacional. De esta forma se apartó también

de la tendencia iberoamericana en esta materia; sin embargo, la Constitución de la República Oriental del Uruguay contiene normas que, sin referirse expresamente a los datos personales, son el fundamento para la protección jurídica de los derechos a la privacidad, a la intimidad, a la autodeterminación informativa, a la protección de los datos personales, a la honra y a la propia imagen en Uruguay. Además, la interpretación de la Constitución en su carácter de normativa en marcadora de los principios generales del derecho permite también una integración de los principios consagrados en tratados internacionales suscriptos por la República Oriental del Uruguay, como parte integrante de su ordenamiento jurídico.

Con esta interpretación iusnaturalista del derecho,la protección de los datos personales está implícita en el ordenamiento jurídico de Uruguay, a partir del texto de los artículos 7, 10, 72 y 332 de la Constitución uruguaya, los cuales, además de establecer una normativa marco en la materia, consagran los principios generales como fuente de derecho.

El artículo 7º de la Constitución uruguaya protege el derecho a la vida y al honor, entre otros derechos fundamentales, pero el artículo 10 es la norma constitucional en la que podemos inferir una mayor relación con el derecho a la autodeterminación informativa, puesto que aun cuando omite mencionar expresamente a los datos personales protege a las personas en su vida privada. Textualmente expresa: "Las acciones privadas de las personas que de ningún modo atacan el orden público ni perjudican a un tercero, están exentas de la autoridad de los magistrados. Ningún habitante de la República será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe". Siguiendo con la enumeración de normas constitucionales, el artículo 72 expresa textualmente que: "La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno".

Además de los preceptos ya mencionados, el artículo 332 expresa que los derechos reconocidos a los individuos por la carta fundamental, no dejarán de

aplicarse por falta de la reglamentación respectiva, la cual deberá ser suplida por los fundamentos de las leyes análogas o los principios generales del derecho y de las doctrinas generalmente admitidas. Es decir, que si aceptamos que la Constitución uruguaya da protección indirecta a los datos de carácter personal, esta protección puede ser planteada judicialmente, en forma operativa, aun a falta de una norma constitucional o infra-constitucional expresa. Dicho de otra forma, podemos expresar que a partir de los mencionados artículos 72 y 332, de la Constitución uruguaya, y hasta tanto no exista una norma constitucional o infraconstitucional expresa, la acción de amparo es el medio idóneo para proteger los datos personales, por su carácter de derecho implícitamente reconocido por la ley fundamental.

De esta forma, con una interpretación amplia de la ley 16.011, que reglamenta el recurso de amparo en Uruguay, podemos encontrar el marco jurídico formal para plantear una acción de habeas data, con fundamento en los artículos antes mencionados, en particular el 72, como remedio genérico para proteger a las personas de los ataques a su intimidad, a su honra, a su imagen, y a sus datos personales.

Además, en este país, existe expresa consagración normativa de la protección de datos personales en normas de alcance sectorial, que vienen a regular distintos aspectos que conciernen a la protección de datos personales y al derecho de acceso. Así podemos mencionar la consagración del secreto tributario y previsional, el secreto bancario, el secreto estadístico, el derecho de acceso a la información, el acceso por la autoridad impositiva a los datos que se encuentren en poder de órganos u organismos públicos estatales o no estatales para el control de los tributos, la acción de amparo, la protección de los datos de identificación civil, la prohibición de cesión, venta, reproducción o entrega a terceros de información relativa al estado civil de las personas del Registro de Estado Civil; la inscripción registral de las personas que tienen la condición de deudor alimentario moroso, el carácter reservado de los datos personales de los menores y adolescentes, los datos médicos, la consagración de la libertad de pensamiento e información, la creación

de un Registro de Empresas Infractoras a la normativa laboral en la órbita del Ministerio de Trabajo y Seguridad Social, etc.

La ley Nº 16.099 sobre libertad de comunicación, de pensamiento e información, conocida como ley de Imprenta, reglamenta el derecho de respuesta en sus artículos 7º a 17º del Capítulo III. A falta de una norma expresa sobre protección de datos personales, los derechos de rectificación y respuesta podrían ser ejercidos a tales efectos, sea que las informaciones provengan de una base de datos o no.

Entre otras normas relacionadas, también encontramos la ley 16.016 que, al regular el Sistema Estadístico de Uruguay sobre los deberes de pertinencia, transparencia, confidencialidad y finalidad, podría ser adoptada para el tratamiento de los datos personales con fines no estadísticos.

Asimismo, el Decreto-Ley Nº 15.322 que regula el Sistema de Intermediación Financiera y sus posteriores reglamentaciones han establecido el secreto bancario en Uruguay. Con igual sentido, el Código Tributario (Ley 14.306), en su artículo 47 obliga a la Administración Tributaria y a sus funcionarios a guardar secreto sobre la información obtenida a partir de una investigación administrativa o judicial. En materia penal, el Código Penal sanciona la violación de correspondencia escrita, telegráfica o telefónica en sus artículos 296 y 297.

Mención especial merece la ley 17.838, titulada "Ley de Protección de Datos Personales para ser Utilizados en Informes Comerciales y *Habeas Data*"[427]. Su artículo primero nos indica que "tiene por objeto regular el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración, y en general, el tratamiento de datos personales asentados en archivos, registros, bases de datos, u otros medios similares autorizados, sean éstos públicos o privados, destinados a brindar informes objetivos de carácter comercial". Como podemos

[427] República Oriental del Uruguay; Ley 17.838. Publicada en el B.O. del 1/10/2004; Nº 26599. Esta ley puede ser consultada en el sitio web del Poder Legislativo de la República Oriental del Uruguay: http://200.40.229.134/leyes/AccesoTextoLey.asp?Ley=17838&Anchor.
Fci: Universitaria: www.fcu.com.uy.

observar, estamos ante una norma de carácter sectorial, puesto que se ocupa sólo de los bancos de datos destinados a brindar informes de carácter comercial. Entendemos que el derecho a la protección de datos personales y a la autodeterminación informativa no puede parcelarse por sectores, y en tanto derechos humanos, su protección debe ser integral por medio de una normativa de alcance general. Pasemos ahora a analizar la ley 17.830:

Con respecto a la legitimación activa, esta ley establece en su artículo 12° que toda persona podrá interponer esta acción y luego el artículo 15° expresamente incluye a las personas jurídicas. A su vez, en caso de personas fallecidas, la legitimación activa se extiende a sus sucesores universales en el artículo 14°.

La ley otorga a los titulares los derechos de acceso, actualización, rectificación, eliminación o supresión de datos. El derecho de acceso surge del artículo 12° y consiste en la posibilidad de toda persona legitimada a entablar una acción efectiva para tomar conocimiento de los datos referidos a su persona, su finalidad y su uso. El derecho de acceso sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que en ese tiempo surgiera un interés legítimo que lo justifique.

Los derechos de actualización, rectificación, eliminación o supresión de datos surgen en caso de error y falsedad en la información del titular o cuando se usen para discriminar o bien sean potencialmente discriminatorios. En tales situaciones, el titular puede exigir la actualización, rectificación, eliminación o supresión de esos datos en forma gratuita. Si el responsable de la base de datos omite realizar los cambios necesarios en sus archivos, en respuesta a lo solicitado por el titular del dato, en un plazo de veinte días hábiles contados desde la fecha en que recibió la solicitud de *habeas data* extrajudicial, se habilita la instancia judicial a los efectos de que pueda interponer una acción judicial de habeas data.

La legitimación pasiva en esta acción recae sobre los bancos de datos o archivos, registros, bases de datos u otros medios similares autorizados, sean

privados o públicos, que realizan tratamiento de datos personales destinados a proveer informes de carácter comercial (artículo 1°). Los sujetos pasivos de esta acción sectorial de *habeas data* son los bancos de datos, en sentido genérico, destinados a proveer informes de carácter comercial.

Con respecto a los datos, la ley autoriza el tratamiento de aquellos datos personales relativos al cumplimiento o no de obligaciones comerciales, que permitan evaluar la conducta comercial o capacidad de pago del titular de los mismos, siempre que sean obtenidos de fuentes de acceso al público o facilitados por el acreedor. En cambio, la ley exceptúa la aplicación de su normativa a aquellos datos que no sean de carácter comercial: por ejemplo a) aquellos que son originados en el ejercicio de las libertades de emitir opinión y de informar, así como aquellos relativos a encuestas o estudios de mercados; b) Datos sensibles, es decir aquellos referentes al origen racial y étnico de las personas, a sus preferencias políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o información referente a la salud física o a su sexualidad y toda otra zona reservada a la libertad individual; c) Datos que no requieren consentimiento, es decir aquellos que: 1) provienen de fuentes públicas de información; 2) son recabados en el ejercicio de las funciones del Estado y 3) son datos de identificación personal (nombre, apellido, DNI, nacionalidad, estado civil, profesión, etc.);

El artículo 5° de la ley establece que los datos almacenados deben ser veraces, adecuados, ecuánimes y no excesivos con relación a la finalidad para la cual fueron obtenidos. En caso contrario, la ley hace responsable al titular o registro del banco de datos.

Con respecto al procedimiento, la ley 17.838 establece que los datos referidos a informaciones comerciales podrán ser registrados por un plazo de cinco años. Si al concluir ese plazo la obligación no ha sido cumplida, el acreedor puede renovar una nueva registración por un plazo similar de cinco años. En caso contrario, si la obligación ha sido cumplida, permanecerán registradas con la expresa mención de

su cancelación durante el tiempo que falte para cumplir los cinco años de registración. En casos de cumplimiento, la registración no puede ser renovada.

Como ya mencionamos, Uruguay ha suscripto pactos y declaraciones internacionales que consagran la protección de la honra, la reputación, la vida privada y familiar y prohíben las injerencias arbitrarias en la vida privada, entre las cuales se encuentran las que se realicen mediante la utilización de datos personales. Estas normas internacionales son derecho positivo vigente en Uruguay, dado que fueron incorporadas por leyes del Congreso al derecho interno.

Sin embargo, a nuestro entender Uruguay necesita legislar una norma específica y de carácter general en materia de protección a los datos personales y a la vida privada de las personas. La ausencia de una norma de tales características en el derecho uruguayo, crea una importante distancia jurídica con el resto del Mercosur, con gran parte de Iberoamérica y en particular con la Unión Europea en materia de protección de datos personales. Estas diferencias en los sistemas jurídicos comparados podrían llegar a impedir la cesión de datos personales con otros Estados, e incluso podría llegar a ser una obstrucción para el desarrollo del comercio en general y del comercio electrónico en particular. No olvidemos que actualmente Uruguay ha crecido considerablemente en sus exportaciones y es una economía en expansión que necesita estar cada vez más conectada con el mundo y transferir datos (muchos de carácter personal) a países que exigen legislaciones equivalentes para permitir la transferencia internacional de datos.

A estudio del parlamento se encuentran dos proyectos de ley que pueden delinear los próximos cambios en el sistema de protección de datos uruguayo. El primero, sobre "Acceso a la información pública y amparo informativo e Instituto Nacional para la información pública"; este proyecto se encuentra a estudio de la Comisión de Educación y Cultura de la Cámara de Senadores desde el año 2006 (Carpeta N° 541/2006). El segundo proyecto, sobre protección de datos, ingresó desde el Poder Ejecutivo al análisis del Poder Legislativo en el mes de septiembre de 2007; se le dio ingreso formal a la Cámara de Senadores en la primera sesión de

octubre y pasó a ser analizado por la Comisión de Educación y Cultura del Parlamento uruguayo.

Desde el año 2010 los referentes políticos uruguayos han comenzado a acordar una nueva reforma a la Constitución, oportunidad en la cual podría debatirse la consagración constitucional del recurso de *habeas data*.

15.- Venezuela

La República Bolivariana de Venezuela ha incluido el habeas data en su Constitucióndel año 2000[428], luego ha realizado una enmienda constitucional el 15 de febrero del año 2009[429], pero a la fecha no ha realizado un desarrollo legislativo infraconstitucional, específico en materia de protección de datos personales.

La Asamblea Nacional Constituyente del año 2000 expresaba en la exposición de motivos de la Constitución que: "Se reconoce por vez primera en el constitucionalismo venezolano, el habeas data o derecho de las personas de acceso a la información que sobre sí mismas o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley. El habeas data incluye el derecho de las personas de conocer el uso que se haga de tales registros y su finalidad, y de solicitar ante el tribunal competente su actualización, rectificación o destrucción, si fuesen erróneos o afectasen ilegítimamente sus derechos".

El mencionado anuncio realizado por la Asamblea Nacional Constituyente del año 2000 en la Exposición de Motivos de la Constitución Bolivariana de Venezuela se concreta en el artículo 28 de la Constitución, dentro del Título III "De los Derechos Humanos y Garantías, y de los Deberes", con el siguiente texto: "Toda

[428] La Constitución de la República Bolivariana de Venezuela fue publicada en la Gaceta Oficial N° 5.453, extraordinario, de 24 de marzo del año 2000. Esta publicación oficial contiene también el texto completo de la exposición de motivos. Véase también: "Constitución de la República Bolivariana de Venezuela". Segunda Edición; Editorial TEMIS S.A., Jurídicas Rincón. Bogotá, pp. 1-350. La Constitución vigente de la República Bolivariana de Venezuela también puede ser consultada en Internet. Fci: Sitio web de la Contraloría General de la Nación: http://www.cgr.gob.ve/contenido.php?Cod=048 (último ingreso 20/2/2012).

[429] Esta enmienda constitucional aprobada el 15 de Febrero de 2009 fue publicada en la Gaceta Oficial de la República Bolivariana de Venezuela el 19 de febrero de 2009, en el Nº 5908.

persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes, consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley". Cabe observar que en este artículo el constituyente omitió nombrar al instituto con el nombre de *habeas data*, denominación que encontraremos más adelante en el artículo 281 inciso 3º. Sin embargo, la Constitución venezolana incorpora en el artículo 28 al *habeas data* informativo -o de acceso a la información-, al *habeas data* de incorporación o adición de datos y al de rectificación y cancelación de datos.

Al analizar el artículo 28 de la Constitución venezolana, observamos que el constituyente mezcló inconvenientemente dos institutos que tienen fines y objetivos diferentes. En la primera parte se incorpora a la Carta Magna venezolana el *habeas data* (propio), bajo la forma de una garantía constitucional para la protección del derecho personalísimo a los datos de carácter personal. En cambio, muy diferente es el instituto consagrado en la segunda parte del artículo 28, el cual nada tiene que ver con la protección de los datos personales. En esta parte del texto se consagra el derecho al acceso libre a la información y documentos que el Estado tenga en su poder y cuyo conocimiento sea de interés para comunidades o grupos de personas. Este instituto también es conocido como derecho a la libertad de información o también algunos autores lo llaman habeas data impropio. Aun así, como ya mencionamos, nada tiene que ver con la protección de datos personales, motivo por el cual es inconveniente la reunión con el habeas data (propio) en un solo artículo.

La explicación de esta última parte del artículo 28 es la copia realizada por el constituyente venezolano del error existente en la mayor parte de las constituciones de Sudamérica, que al consagrar el habeas data buscaron también proteger en el mismo artículo, "el secreto de las fuentes de información periodísticas y de otras profesiones que determine la ley". Insistimos en criticar la inclusión de institutos con naturaleza jurídica y objetivos muy diferentes en un solo artículo de la Constitución. Esta técnica legislativa puede llevar a confusas interpretaciones que priven de claridad a las personas en tanto sujetos de derecho.

La Constitución venezolana atribuye la facultad de interponer las acciones de habeas data, entre otros recursos y acciones de inconstitucionalidad, al Defensor del Pueblo en el artículo 281 inciso 3º. Como mencionamos antes, este es recién el primer lugar en el cual el constituyente menciona a la acción de *habeas data* con este título[430] .

Con relación a la legitimación activa, el constituyente ha legislado que toda persona tiene derecho a acceder a la información, sin ampliarla expresamente a las personas ideales o jurídicas. Esta posibilidad podría abrirse por vía de la legislación de desarrollo o bien por la interpretación de los tribunales de justicia. Por lo tanto, por el momento sólo cuentan con legitimación activa para ejercer la acción de *habeas data*, las personas titulares de sus derechos a la protección de sus datos personales y el Defensor del Pueblo.

La norma constitucional otorga a los legitimados activamente para plantear una acción de *habeas data*, el derecho a acceder a documentos de cualquier naturaleza que contengan información que sobre sí mismos o sus bienes, se encuentre en registros públicos o privados, y que sea de su interés (del titular del dato personal). A su vez, por conducto del *habeas data* impropio o derecho de acceso a la información, reconoce el derecho de toda persona a acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Sin embargo el texto

[430] Basterra, M. (2008). Op. cit., p. 290.

constitucional no establece un proceso especial para la protección de estos derechos, lo que si bien hace que la garantía sea operativa, es inminente la necesidad de una ley que regule el procedimiento.

Efectivamente, más allá de las positivas intenciones del constituyente venezolano, la incorporación del *habeas data* es muy importante, pero no es suficiente para una protección integral de los datos de carácter personal en Venezuela, dado que es necesario un desarrollo infraconstitucional de esta garantía constitucional. Una ley de alcance general que desarrolle el derecho a la protección de los datos personales debe establecer los principios generales del derecho a la protección de los datos personales, debe crear una autoridad de control independiente que vele por el cumplimiento de los derechos otorgados por la Constitución a la futura ley y debe establecer un procedimiento claro para el ejercicio de estos derechos.

Por el contrario, a la fecha sólo observamos algunos desarrollos del precepto constitucional venezolano, pero de alcance sectorial. Un ejemplo de esta política es la Ley de Reforma Parcial de la Ley del Banco Central de la República Bolivariana de Venezuela[431]. Sigue siendo necesaria una norma de alcance general que proteja a las personas en la totalidad de sus datos personales, independientemente de las actividades o sectores de la sociedad en los que actúe.

En materia de protección de datos personales y *habeas data*, el Tribunal Supremo de Justicia de Venezuela, por medio de su Sala Constitucional, ha interpretado que el *habeas data* es una acción constitucional garante del derecho que tiene todo ciudadano de rectificar, actualizar, o destruir la información que resulte lesiva de sus derechos[432] .

[431] Publicada en la Gaceta Oficial de la República Bolivariana de Venezuela el 5 de noviembre de 2009; Nº 39300.

[432] Caso "Carbone Martínez, Pedro Reinaldo c/ Sistema de Información Policial del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas s/ habeas data". Sentencia del Tribunal Supremo de Justicia de la República de El Salvador; Sala Constitucional de fecha 26/6/2006. Fallo citado en: Basterra, M. (2008). Op. cit., p. 292.

16.- El Salvador

La Constitución de la República de El Salvador[433] no incluye al *habeas data*, pero se lo puede considerar implícito en otros artículos de la misma Carta Magna o en Tratados Internacionales a los cuales esta nación se encuentra adherida. A modo de ejemplo podemos mencionar al artículo 2° de la Constitución, cuando protege el derecho al honor, a la intimidad personal y familiar, y a la propia imagen.

La Constitución salvadoreña también establece implícitamente el procedimiento del amparo en el artículo 247, cuando textualmente expresa que ante una violación a los derechos que otorga la Constitución (por ejemplo el ya mencionado artículo 2°), toda persona puede pedir amparo ante la Sala Constitucional de la Corte Suprema de Justicia.

En otras palabras, podemos decir que los derechos reconocidos, tanto implícita como explícitamente por la Constitución, deben ser garantizados a toda persona por el sólo hecho de estar incluidos en la Ley Fundamental, independientemente de que exista o falte una ley reglamentaria o dela naturaleza del legitimado pasivo.

La Sala Constitucional de la Corte Suprema de Justicia tiene jurisprudencia constante en la que establece como requisitos de procedencia básicos para entender en un asunto de *habeas data*, aquellos que se exigen para un amparo: a) la situación de poder en la que se encuentre el responsable del acto lesivo; b) que la acción u omisión que agravia o lesiona al actor sea materia de la Constitución; c) la ausencia de otras vías procesales o administrativas más idóneas de protección frente a actos de la naturaleza denunciada, o que de haberlos sean, ellos insuficientes para garantizar los derechos de los afectados, o bien se hayan agotado plenamente para remediar el acto contra el cual reclama.

[433] Constitución de la República de El Salvador.
Fci.: http://www.constitution.org/cons/elsalvad.htm (último ingreso el 20/2/2012).

Podemos observar que, ante la ausencia de un desarrollo legislativo de la figura del *habeas data* que establezca el procedimiento y los mecanismos de defensa pertinentes, la admisión de la pretensión constitucional relativa a señalar actuaciones que han supuesto afectación al derecho a la autodeterminación informativa, fue receptada en la jurisprudencia salvadoreña a través del procedimiento del amparo.

Sin embargo, la acción de protección de datos personales es una acción de carácter autónomo, con características específicas y presupuestos diferentes a los de amparo, ya que no exige lesión, restricción, acción u omisión de particulares o del Estado. Por este motivo, la jurisprudencia de El Salvador fue adaptando la institución del amparo para reconocer el derecho de las personas a proteger sus datos personales. Así, la Sala Constitucional de la Corte Suprema de Justicia de El Salvador[434] se ha referido al derecho a la intimidad en el ámbito informático, estableciendo que tiene las siguientes implicancias: a) que todo individuo tiene derecho a acceder a la información personal y especialmente a aquella que se encuentra contenida en bancos de datos informatizados; b) que toda persona debe tener la posibilidad y el derecho a controlar razonablemente la transmisión o distribución de la información personal que le afecte; c) que debe existir en el ordenamiento Jurídico, un proceso o recurso que permita hacer efectivos el derecho a la autodeterminación informativa. Como podemos observar, a diferencia del amparo en general, en el reclamo de *habeas data*, aparentemente no hay un derecho lesionado a priori.

El derecho fundamental a la autodeterminación informativa fue reconocido por primera vez en la jurisprudencia salvadoreña durante el año 2004, por vía de la interpretación de la Corte Suprema de Justicia, en un proceso de amparo constitucional que el abogado Boris Solórzano interpuso contra la empresa DICOM, dedicada a recopilar y comercializar información crediticia. Pero, al no existir

[434] Corte Suprema de Justicia de El Salvador.
Fci.: http://www.csj.gob.sv/ (último ingreso el 20/12/2012).

una norma regulatoria del *habeas data*, este proceso sólo puede ser resuelto por la Corte Suprema de Justicia, con la complicación que eso significa.

El 10 de diciembre de 2007 ingresó una nueva demanda de *habeas data* colectiva planteada por INDATA ante la Corte Suprema de Justicia de El Salvador, contra la empresa INFORNET S.A.[435], por comercializar con cuatro millones de datos personales de salvadoreños sin consentimiento de sus titulares y sin control alguno del Estado. La Corte Suprema de Justicia hizo lugar a esta acción de *habeas data* colectiva en sentencia del día 5 de marzo de 2011, en la cual condenó a INFORNET por violar el derecho a la protección de datos o autodeterminación informativa de los salvadoreños mediante el uso y almacenamiento de datos en la base de datoscon fines comerciales de su responsabilidad y titularidad. Además, en el futuro, le prohíbe vender los datos personales sin el consentimiento del titular de los mismos.

Por los motivos expresados, es de suma importancia que El Salvador sancione una ley reglamentaria de la acción de *habeas data*, que contenga una tutela adecuada y efectiva del derecho, un procedimiento de reclamación concreto y una autoridad de control o aplicación de la ley regulatoria.

17.- MERCOSUR

Los Estados fronterizos de Brasil, Argentina, Paraguay y Uruguay, firmaron el Tratado constitutivo del MERCOSUR[436] el 29 de noviembre de 1991, con el objeto de constituir un mercado común con libre circulación de bienes, servicios y factores productivos. El Tratado de Asunción[437], constitutivo del MERCOSUR, proclama ampliamente la "libre circulación de bienes, servicios y factores productivos" entre los países comunitarios (artículo 1º).

[435] Corte Suprema de Justicia de El Salvador; Amparo 934-2007.
[436] MERCOSUR. Fci.: www.mercosur.org.uy/(último ingreso el 21/2/2012).
[437] Tratado de Asunción. Este es el Tratado es constitutivo del MERCOSUR firmado en 1991. Fci.: http://www.mercosur.int/innovaportal/file/655/1/CMC_1991_TRATADO_ES_Asuncion.pdf (último ingreso el 21/2/2012).

Del texto del acuerdo surge para los Estados miembros una amplia libertad de circulación de bienes y servicios que no excluye el flujo de información de ningún tipo, ni siquiera la información de carácter personal. Por ello, es necesario precisar la situación de la información que posee la Administración Pública sobre los administrados en cada país.

El amplio alcance del término "libre circulación de bienes" colisiona con otros marcos de protección de la información, tales como el secreto estadístico, bancario o fiscal u otros institutos de restricción a la libre disponibilidad de los datos en poder de la administración de los Estados miembros.

Entendemos que las normas del Tratado no pueden considerarse derogatorias de tales limitaciones establecidas como garantía de derechos fundamentales.La libre circulación de la información solo es posible en la medida en que no lesione bienes jurídicos más valiosos. No puede considerarse irrestricta, ni pueden entenderse derogadas las normas que protegen y garantizan derechos fundamentales susceptibles de ser agredidos por un intercambio indiscriminado de información.

Ya expresamos, en el Capítulo Primero de esta tesis, que la información no tiene la constitución física de un objeto, recurso o propiedad material; no se encuentra geográficamente atada a nada; es fácilmente obtenible, transmisible, procesable, distribuible, multiplicable y diseminable. A esto se suma el hecho de que en el Derecho internacional todavía no existe un régimen jurídico de la información que regule en forma general el flujo transfronterizo de datos. Determinar un punto medio entre el principio de la soberanía estatal sobre la información y la libertad de información es el gran obstáculo que ha impedido el consenso para una regulación internacional de la información.

El derecho internacional ha tenido un movimiento pendular entre estos dos principios mencionados. Para alcanzar un equilibrio adecuado entre ambos, el Consejo de Europa aprobó en 1973 y 1974 dos resoluciones sobre la protección de la vida privada respecto de los bancos electrónicos existentes tanto en el sector

público como en el privado. Los principios enunciados en esas dos resoluciones fueron el antecedente de las leyes nacionales de protección de datos personales. Sin embargo, al acelerarse el frecuente tráfico de corrientes transfronterizas de datos, gran parte de sus disposiciones fueron burladas y perdieron eficacia. Por esta razón, en 1976 el Comité de Ministros del Consejo de Europa[438] encomendó a un Comité de Expertos la preparación de una Convención para la protección de la vida privada en relación con el procesamiento transfronterizo de datos. A comienzos de 1981 la comisión completó el trabajo y el 28 de enero de ese año se firmó el Convenio para la Protección de las Personas con Relación al Tratamiento Automatizado de Datos de Carácter Personal[439], también conocido como Convenio de Estrasburgo. A la fecha, este Convenio se ha convertido en un modelo para la legislación sobre protección de datos en Europa y más allá de Europa, dado que se encuentra abierto a la firma de cualquier país del mundo. Ha sido ratificado por 43 estados miembros del Consejo de Europa, y con motivo del Día de la Protección de los Datos el 28 de enero, el Consejo de Europa organizó en enero de 2012, reuniones y conferencias para la modernización de esta convención.

Con respecto a las transferencias de datos de carácter personal a través de las fronteras nacionales, el Convenio de Estrasburgo expresa que ninguna de las partes firmantes podrá prohibir o someter a autorización especial los flujos internacionales de datos de carácter personal con destino al territorio de otra parte, a los solos efectos de la protección de la intimidad[440]. Sin embargo, aclara el convenio que cualquiera de las partes firmantes tiene la facultad de dejar sin efecto esta disposición cuando su legislación previere una reglamentación específica para determinadas clases y la naturaleza de bancos de datos de carácter personal, salvo

[438] Consejo de Europa. Op. cit. Fci: http://www.coe.int/lportal/web/coe-portal (último ingreso el 20/2/2012).
[439] Convenio para la Protección de Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, del Consejo de Europa. Op. cit.: Boletín Oficial del Estado (España) N°: 274/1985 del 15 de noviembre de 1985, o en fci.: http://www.judicatura.com/Legislacion/1999.pdf (último ingreso el 22/2/2012).
[440] Art. 13º numeral 2º del Convenio de Estrasburgo: Una Parte no podrá a los solos efectos de la protección de la intimidad prohibir o someter a autorización especial los flujos internacionales de datos de carácter personal con destino al territorio de otra Parte.

que la otra parte proporcionare una regulación normativa que contemple una protección equivalente. O cuando la transferencia se hiciere desde su territorio al territorio de un Estado no contratante, a través del territorio de otra parte, con el fin de evitar que tales transferencias puedan burlar la aplicación de la legislación sobre protección de datos personales de la parte aludida[441].

Los países firmantes del MERCOSUR no han firmado un instrumento que contenga las precisiones del Convenio de Estrasburgo, pero como mencionamos previamente, el Mercosur podría acordar que todos sus Estados miembros se incorporen a esta Convención, dado su carácter de acuerdo internacional abierto.

Pero aún, a falta de textos expresos en los países del MERCOSUR, la información sobre datos personales se encuentra amparada por las normas internacionales y constitucionales que tutelan los derechos del hombre inherentes a su personalidad y garantizan una protección judicial frente a los desbordes del poder.

La acción de amparo es un medio rápido, eficaz y sencillo para lograr la protección de los derechos humanos en general y la protección de los datos de carácter personal en particular, que permita saber qué bases de datos existen y acceder a los datos propios existentes en ellas.

El derecho a exigir la corrección de información falsa o errónea, también puede fundarse en el art. 14 de la Convención Americana sobre Derechos Humanos, más conocida como Pacto de San José de Costa Rica[442]. Esta norma expresa que toda persona afectada por informaciones inexactas o agraviantes emitidas en su

[441] Art. 13º numeral 3º del Convenio de Estrasburgo: "No obstante toda Parte tendrá la facultad de deja sin efecto lo dispuesto en el apartado 2: a) En la medida en que su legislación previere una reglamentación específica para determinadas clases de datos o de archivos automatizados de datos de carácter personal en razón de la naturaleza de tales datos o archivos excepto si la regulación normativa de la otra parte proporcionare una protección equivalente. b) Cuando la transferencia se hiciere desde su territorio al territorio de un Estado no contratante a través del territorio de otra Parte con el fin de evitar que tales transferencias dieran lugar a soslayar la aplicación de la legislación de la Parte aludida al comienzo del presente apartado".

[442] Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica). Op.cit. Fci.: http://www.oas.org/juridico/spanish/firmas/b-32.html (último ingreso el 20/12/2012).

perjuicio y que se dirijan al público en general, tiene derecho a requerir su rectificación.

Más allá de los distintos medios de defensa posibles parece claro que las administraciones nacionales no pueden transferir la información personal de sus administrados irrestrictamente, invocando solamente las normas del Tratado de Asunción, en cuanto al libre flujo de bienes, sin incurrir en responsabilidad. De hecho, la Ley 25.326 de la República Argentina establece que toda transferencia internacional de datos, sólo será permitida, cuando se realice con otro Estado que cuente con un nivel de legislación equivalente (art. 12°).

Recordemos que la República Oriental del Uruguay, a modo de ejemplo, no cuenta con un nivel de legislación equivalente al de la República Argentina, dado que todavía no ha incorporado el *habeas data* a su Constitución y no ha legislado en una norma de alcance general en la materia. Más allá del ejemplo, en general, con respecto al derecho interno de protección de datos personales de cada uno de los miembros del Mercosur nos encontramos con grandes diferencias en el derecho vigente de cada uno de ellos, en materia de protección de datos personales. En un momento en el cual el comercio entre los países integrantes del MERCOSUR está en acelerado crecimiento, estas diferencias normativas pueden transformarse en un gran obstáculo para el comercio electrónico, para la banca y para el sector de los seguros, o bien para la protección del derecho humano a la autodeterminación informativa de sus ciudadanos y habitantes, dados los diferentes niveles de protección a la privacidad que existe en cada Estado miembro.

18.- Cuadro comparativo de algunas normas americanas

País	Constitución *Nº de artículo específico*	Ley específica *Nº de Ley*	Autoridad de control
Argentina	43 ter.	25326	DNPDP
Brasil	223	Hay proyecto	No tiene
Canadá	No tiene	LPRPDE/2000	Comisionado PD
Chile	No tiene	19.628/1999	Registro Civil
Colombia	134	1581/2012	SIC
Bolivia	21, 130 y 131	2631/2004	No tiene
Costa Rica	1111	8968/2011	Prodhab
EEUU	333	Privacy Act /1974	No tiene
Guatemala	111	57/2008	No tiene
El Salvador	No tiene	No tiene	No tiene
Nicaragua	222	LPDP	No tiene
Panamá	202	6/2002	No tiene
Paraguay	135	Ley N° 1682/2001	No tiene
Perú	43	29733/2011	ANPDP
Venezuela	28, 60	No tiene	No tiene
Uruguay	No tiene	17838/2008	No tiene
El Salvador	No tiene	No tiene	No tiene
México	6, 16 y 73	LFPDPPP/2010	IFAI

Aclaración: El cuadro no discrimina entre las autoridades de control que tienen independencia del PE, autonomía y autarquía, de las que no la tienen.

CAPÍTULO IV: PROTECCIÓN DE DATOS EN ARGENTINA

1.- Un nuevo derecho en Argentina

En la República Argentina, el derecho a la protección de los datos de carácter personal comenzó a ser reconocido en el año 1994, al ser incorporado a la Constitución Nacional, luego de la Reforma aprobada ese año.

Cierto es que con anterioridad a la reforma, parte de la doctrina entendía que la ausencia de regulación expresa estaba suplida por vía de los derechos implícitos del art. 33 de la Constitución Nacional, o bien enmarcada dentro del derecho a la privacidad, a través del art. 19 de ese cuerpo normativo fundamental. De todas formas, es recién con esta última reforma constitucional cuando el sistema jurídico argentino incorpora esta garantía constitucional de acción judicial efectiva y el derecho fundamental a la autodeterminación informativa se transforma en derecho positivo[443].

Los reformadores de la Carta Fundamental tomaron como fuente, en este instituto, a la Constitución de Brasil, que en el año 1988 había incorporado el *habeas data* a su texto constitucional. También recurrieron al derecho comunitario europeo, al derecho comparado, a la doctrina de los diferentes autores, nacionales y extranjeros, y a la jurisprudencia en materia de derecho a la intimidad y autodeterminación informativa.

Con estos antecedentes, los convencionales constituyentes de 1994 incorporaron a la Constitución Argentina el art. 43 tercer párrafo, en el cual nacía el *habeas data* argentino.

Posteriormente, surgieron diferentes proyectos de ley para desarrollar el instituto del *habeas data* en una ley específica de protección de los datos de carácter

[443] Basterra, M. I. *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados. Derecho Constitucional Provincial. Iberoamérica y México.* Editorial Ediar – Universidad Nacional Autónoma de México (UNAM). Buenos Aires/México D.F., 2008, p. 62.

personal. Y luego de años de debate, durante el cambio de milenio, en el 2000 fue promulgada la Ley Nacional 25.326 de Protección de los Datos de Carácter Personal.

Esta Ley 25.326 de Protección de Datos Personales tomó como modelo, casi textual, a la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos), Ley española del año 1992[444]. Pero paradójicamente, casi como una trampa cronológica, un año antes, en 1999, España había derogado la LORTAD para promulgar y aprobar la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal).

Luego llegó la creación de la Dirección Nacional de Protección de Datos de Carácter Personal, autoridad en la materia, la jurisprudencia sobre *habeas data* y sobre protección de datos de carácter personal, junto con la reglamentación de la nueva ley.

En la actualidad es necesario continuar el estudio del *habeas data* y del derecho a la protección de los datos de carácter personal, desde sus antecedentes hasta sus últimas evoluciones, dado que el objeto jurídicamente protegido por estas normas se encuentra cada día más amenazado y vulnerable por la acelerada evolución tecnológica. Pensemos solamente en los conflictos jurídicos que puede causar la acumulación de datos personales por tele vigilancia, por asignación de una tarjeta obligatoria de transporte, por adhesión a una red social con incorporación de fotografías personales y familiares, junto a un largo etcétera.

2.- Intimidad y datos personales en la historia argentina

Si hacemos un poco de historia, encontramos que desde los tiempos coloniales, los gobiernos del Río de la Plata mantuvieron el monopolio estatal de la registración de datos de la vida y de las propiedades de los súbditos del Estado[445].

[444] La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos. Op. cit., España.
[445] Pierini, A.; Lorences V.; Tornabene, M. *Habeas Data. Derecho a la Intimidad*. Editorial Universidad. Buenos Aires, 1998, p. 65.

La información estuvo en poder de una minoría aristocrática, que mantuvo al resto de la población en un estado de desinformación planificada.

A partir de 1810 se realizaron distintos intentos de organización institucional que desembocaron en la declaración de la independencia de Tucumán en 1816 y en distintos proyectos constitucionales[446] (1813, 1819 y 1826). Este proceso se frenó a partir de 1830, cuando Argentina entró en un prolongado proceso de tiranía, marcado por la llegada al poder de Juan Manuel de Rosas, quien instauró un Estado inquisidor[447] que llevó adelante un control absoluto de las personas y de sus datos personales.

La caída de Rosas, en 1852, permitió la promulgación de la Constitución Argentina (1853). En la Carta Magna no se mencionaron las palabras intimidad ni privacidad, pero la doctrina y la jurisprudencia les han reconocido a estos derechos un rango constitucional, a partir de la protección que el artículo 19 otorga a las acciones privadas de los hombres[448], junto a la inviolabilidad del domicilio, de la correspondencia y de los papeles privados (art. 18º de la C.N.).

Hasta poco antes de la promulgación de la actual ley de protección de los datos de carácter personal (año 2000), la jurisprudencia ha respondido afirmativamente a la aplicación de los artículos 18 y 19 para amparar los derechos a la intimidad y a la protección de los datos personales, y de ser necesario, ordenar la rectificación y cancelación de registros que atenten contra estos derechos.

A partir de 1930[449], se iniciaron tiempos de alternancia entre gobiernos democráticos y de facto, durante los cuales el respeto por los derechos fundamentales estuvo ausente. Los derechos de la persona fueron vulnerados en

[446] Romero, J. *Breve historia de la Argentina*. Editorial Fondo de Cultura Económica de Argentina. Buenos Aires, 1996, p. 54.
[447] Luna, F. *Breve Historia de los Argentinos*. Editorial Planeta Argentina. Buenos Aires, 2000, p. 91.
[448] Artículo 19 de la Constitución Argentina: "Las acciones privadas de los hombres, que no ofendan al orden y a la moral pública, ni perjudiquen a un tercero, solo están reservadas a Dios y exentas de la autoridad de los magistrados".
[449] El gobierno militar finalizó, en Argentina, en el año 1983 con el regreso de la democracia y la llegada de Raúl Alfonsín a la Presidencia de la Nación.

toda su extensión durante los períodos de interrupción democrática, que se sucedieron a partir del primer golpe de Estado (en el año 1930). Pero tampoco fueron resguardados durante gobiernos constitucionales y cuasi democráticos que alternaron en este período aciago.

Un nuevo período democrático llegó a la Argentina con la elección del Presidente Raúl Alfonsín en el año 1983; con este cambio político se sintió una sensación de tolerancia y pluralismo que aportó el contexto histórico para reflexionar sobre los derechos humanos y fundamentales de las personas.

La influencia del derecho comparado generó en 1985, las condiciones para que la Corte Suprema de Justicia definiera con amplitud el contenido del derecho a la intimidad en el caso Ponzetti de Balbín, Indalia c/. Editorial Atlántida[450]. El fallo reconoce el derecho a la intimidad y a la propia imagen, con fundamento en el artículo 19 de la Carta Fundamental, y encuentra en esos derechos una relación directa con el derecho a la libertad personal, que protege jurídicamente un ámbito de autonomía individual, constituido por los sentimientos, hábitos, costumbres, relaciones familiares, situación económica, creencias religiosas, salud mental, salud física, acciones, hechos o actos que quedan reservados al propio individuo.

La Corte Suprema de Justicia de la Nación[451] ha manifestado que el mencionado artículo 1071 bis es consecuencia del derecho fundamental a la privacidad, consagrado en el artículo 19 de la Carta Magna, como también en el Pacto de San José de Costa Rica (Adla, XLI-b, 1250). El mencionado acuerdo establece que toda persona tiene derecho a la protección de la ley contra injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación[452].

El Código Civil Argentino también atendió la protección del derecho a la intimidad de las personas en el artículo 1071 bis del Código Civil, donde prohíbe

[450] Ponzetti de Balbín, Indalia c/ Editorial Atlántida S.A.; C.S. 1984/12/11. La Ley 1985 –B- 114.
[451] Corte Suprema de Justicia de la Nación Argentina. Fci.: www.pjn.gov.ar.
[452] *Caso Ponzetti de Balbín, Indalia c/ Editorial Atlántida S.A. C.S., 1984/12/11*. Editorial La Ley. Suplemento Universitario La Ley. Buenos Aires, 2001, p.4.

que alguien se entrometa en forma arbitraria en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad. La norma expresa que quien realizare ilegalmente estas acciones, deberá pagar una indemnización que habrá fijado el juez[453], quien también podrá, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación.

En esta norma observamos un compromiso con la protección de la intimidad de las personas en el derecho positivo argentino, al ordenar que todo aquel que arbitrariamente se entrometa en la vida ajena cese de realizar actividades. Este artículo fue incorporado al Código Civil por la ley 21.173[454] publicada en el Boletín Oficial el 2/10/1975, de carácter general y de amplio contenido para establecer la responsabilidad y el cese de toda actividad que implique intromisión en la vida ajena, preservando la imagen, la correspondencia y perturbaciones referidas a los sentimientos, costumbres, creencias y a la intimidad. Su caracterización indica que más allá de la posible acción penal, o paralelamente a ella, existe responsabilidad civil por la realización de cualquiera de los actos lesivos en cuestión. La enumeración contenida en el mencionado artículo debe interpretarse como meramente enunciativa respecto de las conductas prohibidas.

La jurisprudencia de la Cámara Civil y Comercial de Mercedes[455] (Prov. de Buenos Aires) entendió que "El art. 1071 bis del Código Civil veda la turbación de la vida privada, por lo que el quid de la cuestión no está en que se tome conocimiento, ya que cualquiera puede tomar conocimiento, incluso en forma

[453] Artículo 107l bis del Código Civil argentino: "El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otro en sus costumbres o sentimientos o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente un juez, de acuerdo con las circunstancias; además podrá este a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación".

[454] Ley 21173. Fci.: http://federacionuniversitaria21.blogspot.com/2008/08/ley-21173-derecho-la-intimidad.html (último ingreso el 23/2/2012).

[455] Cámara Civil y Comercial de Mercedes, Sala II, Mayo 6 de 1997, "F., N.N. c/ Semanario Reseña y otros" (jurisprudencia), LLBA, 1997-881.

casual, de aspectos de la vida privada de otro, sin por ello violar la intimidad de este, lo que prohíbe es invadir esa esfera privada de la personalidad en la cual tiene la persona derecho a desenvolverse sin que la indiscreción ajena tenga acceso a ella, aunque se trata de actos o acciones no desplegadas en ámbitos privados, es decir la divulgación, por medio de la prensa, de datos que por su naturaleza están destinados a ser preservados de la curiosidad pública, dentro de la cual tiene cabida el derecho al anonimato".

La expresión "vida ajena" que usa el art. 1071 bis del C.C. implica una intromisión en la intimidad y un avance sobre los derechos personalísimos de la persona afectada. La actividad ilegítima se refiere a la persona, su imagen, su dignidad, sus creencias, ideología, documentación privada, y debe implicar necesariamente una perturbación de cualquier tipo. El requisito de la perturbación o molestia es el elemento constitutivo del accionar prohibido.

La legitimación activa para esta acción recae en la persona afectada, único posible accionante, ya que es solo él quien puede evaluar el grado de afectación personal que ese hecho le representó, así como el interés en accionar y los alcances de la pretensión.

A partir de la reforma constitucional de 1994, se incorporó en nuestra Carta Magna una nueva garantía constitucional para proteger los datos personales y la autodeterminación informativa de las personas. La incorporación de estos nuevos derechos humanos de tercera generación en la Constitución Argentina se produce como consecuencia de una importante evolución del derecho a la intimidad en el derecho comparado. Sin embargo, el Código Civil argentino no ha legislado en forma expresa sobre la protección de los datos de carácter personal, aun cuando fue tratado en los siguientes proyectos de reforma:

El Proyecto de Unificación de la legislación civil y comercial de 1987[456], consagraba expresamente la reparación de los daños sufridos por las personas de existencia visible en sus derechos a la intimidad personal y familiar y al respecto de su honra y reputación; limita la acumulación de información nominativa en registros informatizados, salvo consentimiento expreso del interesado o autorización legal y previa; se establece el derecho del sujeto cuyos datos sean acumulados, de verificar su amplitud y tenor, exigiendo su corrección y actualización y su utilización conforme a la finalidad para la cual fueron recogidos, y se prohíbe dar a conocer a terceros dichos datos sin conformidad expresa del interesado o disposición legal que lo autorice (artículos 110 al 116).

En 1992 el Poder Ejecutivo Nacional intentó nuevamente reformar el Código Civil, mediante la designación de una comisión de reconocidos juristas para la redacción del proyecto de nuevo Código Civil. El Decreto 468/92 del PEN, por el cual se designaba la mencionada comisión[457], aludía a aspectos centrales de la protección de datos personales en la sugerida reforma al Libro II del Código Civil.

Por último, el proyecto de Código Civil de la República Argentina unificado con el Código de Comercio redactado por una Comisión designada en el año 1995 a través del Decreto 685/95[458] ha dejado un vacío legal en lo referente a la protección de datos personales. Aun así, este proyecto incluyó un apartado referido a los derechos a la personalidad. Y dentro de este capítulo, el proyecto estatuye una acción civil para reclamar la reparación de los daños sufridos a toda persona

[456] Proyecto de ley de la Cámara de Diputados de la Nación (año 1987), preparado por una Comisión Honoraria integrada por los Doctores Héctor Alegría, Atilio Aníbal Alterini, Jorge Horacio Alterini, Miguel Carlos Araya, Francisco A. de la Vega, Horacio P. Fargosi, Sergio Le Pera y Ana Isabel Piaggi; el Senado Nacional sometió el trabajo al análisis de una Comisión Técnica Jurídica, que presidió el Dr. Luis Moisset de Espanés, a quien acompañaron los Doctores José L. García Castrillón, Fernando J. López de Zavalía, Luis Niel Puig, Juan Carlos Palmero, Juan F. Ravignani, José D. Ray, Adolfo M. Rodríguez Saa, Mario C. Russomanno, Carlos Suárez Anzorena, Ernesto Clemente Wayar y Eduardo A. Zannoni.

[457] Esta comisión estaba integrada por los Doctores Belluscio, Berrgel, Kemelmager de Carlucci, Le Pera, Rivera, Videla Escalada y Zannoni.

[458] Esta Comisión estuvo integrada por los Doctores Alegría, Atilio Alterini, Jorge Alterini, Mendez Costa, Rivera y Roitman.

humana afectada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal[459].

Actualmente Argentina discute un nuevo proyecto de Código Civil y Comercial de la Nación[460] que se encuentra en avanzado debate en el Congreso de la Nación. En este proyecto de nueva codificación encontramos en el Libro Primero (Parte General), Título I (Persona Humana), Capítulo 3 (Derechos y actos personalísimos), normas sobre la inviolabilidad de la persona humana (art. 51) y sobre las afectaciones a la dignidad (art.52). El artículo 52 expresamente dice: "La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos, conforme lo dispuesto en el Libro Tercero, Título V, Capítulo I."

Podemos observar que en el artículo comentado no se incluyen a los datos personales, sin embargo entendemos que en atención a la evolución del derecho a la autodeterminación informativa en Argentina y el mundo, la protección a los datos personales también debería estar contemplada en ese artículo del proyecto[461].

El 6 de septiembre de 2012 se realizó en la ciudad de San Miguel de Tucumán un Audiencia Pública sobre la reforma del Código Civil y Comercial, convocada por la Comisión Bicameral del Congreso de la Nación. En esa oportunidad presentamos ponencia proponiendo la incorporación de la protección

---

[459] Art. 105 del Libro segundo de la Parte General; Título Primero "De la Persona Humana"; Capítulo VI del Proyecto de Código Civil de la República Argentina unificado con el Código de Comercio de 1995.

[460] Proyecto del Poder Ejecutivo de la Nación redactado por la Comisión de Reformas designada por decreto 191/2011. Ricardo Luis Lorenzetti (Presidente), Elena Highton de Nolasco y Aída Kemelmajer de Carlucci. Fci.: www.nuevocodigocivil.com
Código Civil y Comercial de la Nación. Proyecto del Poder Ejecutivo de la Nación redactado por la Comisión de Reformas designada por Decreto 191/2011. Presentación del Proyecto por Ricardo Luis Lorenzetti. Editorial Rubinzal – Culzoni, Santa Fe, 2012.

[461] De *lege ferenda* proponemos el siguiente articulado: "La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, **datos personales y autodeterminación informativa** o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos, conforme lo dispuesto en el Libro Tercero, Título V, Capítulo I."

de datos personales y del derecho a la autodeterminación informática en el artículo 51 del proyecto de reforma[462].

En el sistema jurídico argentino existen sanciones penales para quien afectare el derecho a la intimidad de las personas. Los delitos de violación de domicilio (art. 151) y de secretos (art. 133 a 157) están tipificados en el Código Penal desde antes de la promulgación de la ley 25326. La ley de Protección de Datos Personales N° 25.326, incorporó dos nuevos delitos directamente relacionados con la protección de los datos de carácter personal en los artículos 117 bis y 157 bis del Código Penal, donde se encuentran los tipos penales correspondientes al hacker de datos personales y al cracker de los datos personales.

En el año 2008, por medio de los artículos 8° y 14° de la ley 26.388 de Delitos Informáticos, se derogó el inciso 1° del artículo 117 bis y se lo trasladó al 157° bis, que en su nueva redacción quedó con el siguiente texto: Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno (1) a cuatro (4) años.

En el derecho societario también se incorporó la protección de los datos personales, por medio del derecho a la intimidad de las personas jurídicas, prohibiendo que las entidades financieras[463] revelen la información que reciban de sus clientes o los datos sobre operaciones financieras que estos realicen.

---

[462] Audiencia pública realizada en la ciudad de San Miguel de Tucumán sobre la reforma del Código Civil argentino. En este sitio pueden consultarse las ponencias, los videos y las versiones taquigráficas de las comunicaciones presentadas ante la Comisión Bicameral de Reforma del Código Civil. Fci.: http://ccycn.congreso.gov.ar/convocatoria/06-09.html.

[463] Argentina; art. 39 de la ley de Entidades Financieras Nº 21.526.

Hasta el año 1994, la Constitución Argentina protegía indirectamente a los datos de carácter personal por medio de los artículos 19 y 33. El artículo 19 expresa que las acciones privadas de los hombres que no ofendan al orden, la moral pública, ni perjudiquen a un tercero están exentas de la autoridad de los magistrados. El art. 33 busca proteger los derechos naturales aún no reconocidos por la Constitución; este artículo estatuye que las declaraciones, derechos y garantías que enumera la Constitución, no serán entendidos como negación de otros derechos no enumerados, que nacen del principio de soberanía del pueblo y de la forma republicana de gobierno.

Puede observarse que el art. 33 se vincula en forma directa con la facultad del Congreso de la Nación de aprobar o desechar tratados con las demás naciones, con los organismos internacionales y concordatos con la Santa Sede (inciso 22 del art. 75 de la Constitución Nacional). La enumeración realizada por el artículo 33 tiene un contenido implícito referido a todo tipo de situación que se vincule con los acuerdos internacionales que menciona el inc. 22 del art. 75 de la Constitución y con los tratados futuros que a pesar de no estar expresamente individualizados en la Constitución gozarán de la jerarquía de ley suprema de la nación. Estos acuerdos aluden a derechos civiles, derechos políticos, derechos económicos sociales y culturales, pero no se agotan en ello, sino que mantienen su contenido para situaciones derivadas, implícitas o no debidamente enunciadas en el texto constitucional.

3.- Reforma constitucional de 1994

A fines del año 1993, en un momento de relativa paz social y calma económica, el entonces presidente Carlos Menem acordó con el ex presidente Raúl Alfonsín un acuerdo político para la promulgación de una reforma constitucional que fortaleciera las instituciones republicanas[464]. Menem buscaba incorporar al

[464] Romero, J. (1999). Op. cit., p. 203.

texto constitucional la re-elección presidencial; Alfonsín, la figura del Jefe de Gabinete dentro de la estructura funcional del Poder Ejecutivo.

En un principio las intenciones de estos dos líderes de los partidos políticos, más importantes de la República Argentina, se dirigían a incorporar más derechos políticos para los políticos Sin embargo, conocedores de la sociedad argentina, comprendieron que para alcanzar consensos necesitaban diluirsus intereses con la incorporación de nuevos derechos para las personas: de esta forma el *habeas data*emergió como uno de los nuevos derechos sobre los que debatió el impulso reformador.

Con esta impronta se aprobó la reforma en 1994[465]. Entre las diferentes modificaciones e incorporaciones incluyó la acción de amparo en el artículo 43 y dentro del marco de esta acción, en su tercer párrafo, se incorpora al instituto del habeas data en Argentina, aun cuando expresamente no se le da ese nombre.

Estamos ante una acción *habeas data* innominada, que aparece como una garantía constitucional que otorga a las personas una acción judicial de protección de sus datos personales. Garantiza el acceso y el conocimiento de los datos personales existentes en registros, archivos o bancos de datos, y en caso de que esos sean falsos o tengan una función discriminatoria, también es útil para corregir o eliminar dicha información o exigir su confidencialidad.

El texto del art. 43, 3er párrafo, de la Constitución reformada en 1994, decreta que toda persona podrá interponer una acción, expedita y rápida, para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros y bancos de datos públicos, o los privados destinados a proveer informes; y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. Agrega que no podrá afectarse el secreto de las fuentes de información periodísticas.

---

[465] Constitución de la República Argentina con sus reformas de 1994. Fci.: http://www.senado.gov.ar/web/constitucion/cuerpo1.html.

3.1.- Doctrina y jurisprudencia

Los comentarios doctrinarios y las decisiones jurisprudenciales, ejercieron su influencia y moldearon esta garantía constitucional contra la violación del derecho a la autodeterminación informativa.La jurisprudencia aplicó el art. 43, tercer párrafo, de la Constitución reformada para resolver las cuestiones planteadassobre datos personales; entre ellos se destaca el fallo de la Corte Suprema de Justicia de la Nación Argentina, en el caso Urteaga, Facundo Raúl c/ Estado Mayor Conjunto de las Fuerzas Armadas s/ amparo - ley 16.986; por el cual hace lugar al *habeas data* planteado por el hermano de un desaparecido en un Recurso Extraordinario y revoca la sentencia de la Sala II de la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal[466].

En octubre del año 1996, la Cámara de Apelaciones en lo Contencioso Administrativo de la Capital Federal rechazó una demanda de *habeas data* por la que el actor buscaba acceder a información sobre su hermano desaparecido, la que obraría en bancos de datos de organismos del gobierno nacional y de la provincia de Bs. As. La sala sostuvo que "...el actor carece de legitimación para intentar la presente acción en tanto los datos que pretende recabar no están referidos a su persona...".

Luego del rechazo en primera y en segunda instancia de una acción de habeas data para obtener información de los bancos de datos del Estado sobre su hermano desaparecido en julio de 1976 en la Provincia de Buenos Aires durante el gobierno militar (1976-1983), Facundo Urteaga planteó, en 1998, un recurso extraordinario ante la Corte Suprema de Justicia de la Nación.

Con un criterio ajustado a la interpretación del instituto en el derecho comparado, la Cámara Nacional de Apelaciones había rechazado esta acción de habeas data, en atención a la falta de legitimación activa del actor, dado que los

[466] Sentencia del caso "Urteaga, Facundo Raúl c/ Estado Mayor Conjunto de las Fuerzas Armadas s/ amparo - ley 16.986", (Argentina: Jurisprudencia).
Fci.: http://www.planetaius.com.ar/fallos/jurisprudencia-u/caso-Urteaga-Facundo-Raul-c-Estado-Nacional-Estado-Mayor-Conjunto-de-las-FF-AA.htm (último ingreso el 24/2/2012).

datos que pretendía recabar no se referían a su persona, sino a la de su hermano. Sin embargo, la Corte Suprema entendió que el tribunal de origen aplicó un excesivo rigor formal que deja sin protección el derecho invocado por el recurrente, aun cuando la pretensión no era ajena al propósito del constituyente, y con estos argumentos concedió la acción de habeas data planteada por Facundo Urteaga.

La interpretación realizada por la Suprema Corte de Justicia rompió con la concepción de derecho personalísimo atribuida en forma unánime a la protección de los datos de carácter personal en la doctrina y jurisprudencia internacional. Este antecedente jurisprudencial gravitó posteriormente en la discusión y sanción de la ley 25.326 sobre protección de los datos personales, para otorgar legitimación activa a los familiares del titular de los datos.

Hay autores que entienden que, en la medida en que se vea afectada esa "intimidad familiar", cabe aceptar el habeas data ejercido para corregir información falsa o discriminatoria sobre el causante, existente en un registro o banco de datos.

3.2.- *Habeas Data*: naturaleza jurídica y trámite procesal

El constituyente de 1994 dio al *habeas data* el molde del amparo[467]. Desde el año 1994 hasta el año 2000[468]no existió una ley que reglamentara su desarrollo, y dada su naturaleza operativa, se tramitó siguiendo las reglas procesales del amparo[469].

Antes de la sanción de la ley 25.326, la doctrina debatió largamente sobre la naturaleza jurídica de la acción de *habeas data* consagrada por la Constitución Nacional. Los prestigiosos autores de la doctrina jurídica argentina: Sagués, Quiroga Lavié y Víctor Bazán, entienden que se trata de una variable de la acción

[467] Sbdar, C. (Directora y Coordinadora) *Estudio del Amparo en la Nación y en la Provincia de Tucumán. Competencia – Admisibilidad – Trámite – Recursos – Cosa Juzgada*. Capítulo III. Trámite del Amparo: Ciolli, M.; Juarez Peñalba, C.; Paz, A.; Spiner, S. Editorial ER Ediciones del Rectorado. Universidad Nacional de Tucumán. 2006, p. 98.
[468] En el año 2000 entró en vigencia la ley 25326 que desarrolló al habeas data.
[469] Pierini, A.; Lorences V.; Tornabene, M. (1998). Op. cit., p. 78

de amparo. Sin embargo, hoy, luego de la entrada en vigencia de la ley de protección de datos personales, no queda duda de que estamos ante un proceso autónomo, dado que expresamente la ley 25.326, determina las particularidades de un proceso diferente, determinado legalmente para la acción de protección de datos personales.

La acción de *habeas data* también integra el plexo de garantías de la Constitución, tomando como fundamento la búsqueda del equilibrio entre dos derechos en juego: el derecho del Estado y de las entidades privadas de acumular información relativa a las personas, frente a un derecho no menos importante, incluso superior: el derecho de esas mismas personas a la preservación de su intimidad.

Erróneamente, la acción de *habeas data* se encuentra limitada por la garantía constitucional a la intangibilidad de las fuentes de información periodísticas, ya que la protección de las fuentes periodísticas nada tiene que ver con la protección de los datos personales. Sin embargo, el jurista argentino Quiroga Lavié opina en contrario y propicia que la protección a las fuentes de información periodística sea ampliada a otras actividades profesionales implicadas por el secreto, tales como el servicio profesional de médicos, religiosos, abogados, y demás actividades obligadas a recibir informaciones reservadas o secretas.

Cabe observar que la obligación de secreto profesional nada tiene que ver con la protección de los datos de carácter personal. Y en el hipotético caso de colisión entre estos derechos, la Constitución debe dar prioridad a la protección del dato personal por su estrecha y directa relación con el derecho personalísimo, humano y de tercera generación a la intimidad que tenemos todas las personas. Por estos motivos habría que eliminar el agregado, referido a la protección a las fuentes periodísticas, del artículo 43 tercer párrafo, dado que en él se hace expresa referencia al acceso a los “bancos de datos destinados a proveer informes”, y este no es el caso de las fuentes de información periodística, ni de la información recibida

por sacerdotes, médicos, abogados, etc. Retacear la protección a los datos personales es un desacierto constitucional.

La mayoría de los autores de la doctrina y la jurisprudencia argentina coinciden en afirmar que la acción de habeas data busca proteger el derecho a la intimidad, ya que la indefensión de la persona frente al mal uso de sus datos y a la publicidad de los mismos afecta sus derechos constitucionales a la privacidad. La protección de los datos de carácter personal es un derecho humano de tercera generación, que surge frente a la necesidad de una protección adecuada de la intimidad ante el desmedido avance de las tecnologías de la información. La Constitución incluye la acción de *habeas data*, en su plexo de garantías, con el propósito de evitar que mediante el uso de la informática se pueda lesionar el honor o la intimidad de las personas.

El *habeas data* protege un "complejo de derechos personalísimos", que incluyen la intimidad, la privacidad y la identidad de las personas.

El derecho a la identidad es la forma en que una persona desea presentarse a la sociedad o a terceros. El objeto de la acción de *habeas data* también incluye la protección de este derecho a la identidad de las personas, ya que, cuando los datos personales divulgados por un banco de datos son datos sensibles, se daña y afecta el derecho a la identidad personal. Del mismo modo que, cuando una persona pretende corregir información falsa o discriminatoria almacenada en un banco de datos público o privado y que es difundida a terceros, lo que busca principalmente es tutelar la identidad que posee frente a la sociedad.

Tanto el derecho a la intimidad como el derecho a la identidad son derechos personalísimos que encuentran su fundamento en el reconocimiento del valor que las personas tienen en sí mismas. Además, al requerir el texto constitucional la existencia de falsedad o discriminación como requisitos para la procedencia de la acción de *habeas data*, busca preservar los valores "verdad" e "igualdad", con

relación a la información sobre la identidad de las personas, almacenada en registros o bancos de datos.

En Argentina, la jurisprudencia ha conceptualizado un doble objetivo en la acción de *habeas data*, de acuerdo con su finalidad. Por un lado, la posibilidad de que toda persona tome conocimiento de los datos a ella referidos que consten en registros o bancos de datos públicos o privados y de su finalidad, y por el otro, en caso de falsedad o discriminación, se otorga el derecho para exigir su supresión, rectificación, confidencialidad o actualización.

Estamos ante un derecho de la persona a controlar los datos e informaciones que otros tienen sobre ella y que hacen a su identidad, su personalidad y sus hábitos, aspectos que delimitan el objeto o finalidad del *habeas data*.

La acción de habeas data contemplada por el artículo 43, tercer párrafo, de la Constitución Nacional es una norma que reviste carácter operativo, motivos por los cuales cualquier persona que se considere afectada, puede hacer valer sus derechos, aún a falta de ley o decreto reglamentario que la desarrolle o reglamente. En este sentido, la Corte Suprema sostuvo que una norma es operativa cuando está dirigida a una situación de la realidad en la que puede operar inmediatamente, sin necesidad de reglamentación alguna, lo que no quiere decir que prohíba esa reglamentación, sino que tan solo no es imprescindible, ya que el derecho a la protección de los datos personales tiene virtualidad propia.

3.2.1.- Legitimación activa en la acción de *habeas data*

Con respecto al legitimado activo para plantear una acción de *habeas data*, el tercer párrafo del art. 43 CN autoriza a toda persona, a tomar conocimiento de los datos a ella referidos. Ello implica que su ejercicio es de carácter personal, restringido sólo al afectado, a diferencia de lo que sucede con el *habeas corpus*, concedido al afectado o a cualquiera en su favor.

En sus primeros años, la doctrina interpretó que la acción de *habeas data* no era una acción popular y que solo podía ser articulada por el afectado. Sin embargo, en la actualidad han surgido opiniones diferentes y, además, la jurisprudencia extranjera ha receptado el *habeas data* colectivo[470] y las acciones de clase[471].

Para algunos autores, el *habeas data* busca solamente que el particular damnificado tome conocimiento de los datos a él referidos y su finalidad. En consecuencia, no es una acción útil para tomar conocimiento de datos de terceros, o información de otro tipo, materia del derecho al acceso a la información pública, lo que también es llamado por algunos autores, *habeas data* impropio.

En este sentido, Osvaldo Gozaíni entiende que esta acción genera por su propia naturaleza la idea de un proceso propio, particular, donde el afectado es la persona o la empresa que sufre un perjuicio por el uso impropio de la información que le concierne. Una demanda de *habeas data* busca acceder a la base de datos para conocer los datos referidos al actos, los errores que pudieren existir, el origen de esos errores, la existencia de un consentimiento previo o legalidad del almacenamiento de esos datos, y de ser necesario para solicitar la actualización, rectificación, supresión o confidencialidad de los mismos. Por este motivo, Gozaíni ve incierta la posibilidad de interceder acciones colectivas destinadas a un objeto preciso sobre alguna de estas pretensiones posibles en el *habeas data.*

Sin embargo, el autor citado expresa que la posibilidad del *habeas data* colectivo se abre cuando en lugar de observar a la persona que solicita, se hace foco en el objeto que se quiere preservar, y en este aspecto, cuando son los datos en su género los que están afectados, la vía adecuada sería el proceso constitucional colectivo, sin que sea una acción popular. Para llegar a este planteo, establece cierta distinción entre el derecho de acceso y el proceso judicial que regula la ley 25.326,

[470] Ver capítulo III de estos estudios, p. 323 sobre el derecho a la protección de datos personales en la República de El Salvador.
[471] CSJN (Argentina). Op. cit. Fci: "Halabi, Ernesto c/ P.E.N. - ley 25.873 - dto. 1563/04 s/ amparo ley 16.986". Fallo del 24 de Febrero de 2009: http://www.iprofesional.com/notas/78867-Fallo-Halabi-Ernesto-c-PEN---ley-25873---dto-156304-s-amparo-ley-16986.html (último ingreso el 26/2/2012).

que comentaremos más adelante. Y encuentra factible una acción colectiva planteada dentro del proceso judicial, dado que mientras el derecho de acceso se otorga al titular de los datos, que debe acreditar su identidad para tener la posibilidad de obtener información directa de los archivos públicos o privados destinados a proveer informes, mientras que la demanda judicial puede enderezar la pretensión a cualquiera de las acciones de rectificación, supresión, confidencialidad o actualización, cuando de ellos se hace un tratamiento discriminatorio genérico o de alcances a un grupo o sector particular[472].

Con respecto a la legitimación activa de las personas jurídicas, entendemos que al no haber distinción en el texto constitucional, se posibilita su ejercicio tanto a personas individuales como colectivas, pues donde la ley no distingue, el intérprete tampoco debe hacerlo. Tratándose de una persona jurídica, no será el derecho a la intimidad el que esté afectado, pues este último no es posible predicarlo de aquellas, aunque sí puede hablarse de un derecho a la identidad o a la buena imagen de las personas jurídicas que se proyectan en el nombre comercial o en el valor del fondo de comercio o en la marca de sus productos y el prestigio que estos tienen, por señalar algunos ejemplos.

Además, siguiendo la definición del Código Civil, "persona es todo sujeto susceptible de adquirir derechos y contraer obligaciones", por lo que debe entenderse que comprende tanto a las personas físicas como personas jurídicas, con el alcance del art. 33 del Código Civil. En la práctica, los tribunales han aceptado como actores en los procesos de habeas data a las personas jurídicas, aun antes de la entrada en vigencia de la ley 25.326, que las considera legitimadas procesalmente en forma activa.

[472] Gozaíni, O. (2011). Op. cit., p. 539.

3.2.2.- Legitimación pasiva en la acción de *habeas data*

La Constitución Nacional expresa en el artículo 43, tercer párrafo, que la acción de *habeas data* puede ser planteada contra todo banco de datos público o privado destinado a proveer informes. En otras palabras, los legitimados pasivos del instituto del *habeas data* de la Constitución Nacional, son todos los bancos de datos personales, tanto aquellos que funcionan en el sector privado, como aquellos que dependen del Estado Nacional, Municipal o Provincial.

4.- Desarrollo normativo del artículo 43 ter.

Una vez que entró en vigencia la Constitución reformada en 1994, fue necesario desarrollar legislativamente el mandato constitucional de art. 43, tercer párrafo. Existió primero un intento frustrado (la vetada ley 24.745) y finalmente, en el año 2001, se aprobó la ley vigente Nº 25326 en Argentina.

4.1.- La vetada ley sobre *habeas data* N° 24.745

Posteriormente, el Congreso Nacional, por proyecto iniciado en el Senado de la Nación, sancionó durante la presidencia de Carlos Menem, en diciembre de 1996, la ley N° 24.745, conocida como "Ley de *Habeas Data*" por medio de la cual desarrollaba el tercer párrafo del art. 43 de la Constitución Nacional. Esta ley fue sancionada luego de un largo proceso de enfrentamiento entre las dos cámaras legislativas. Sin embargo, luego de mucha polémica, esta ley fue vetada totalmente por el Poder Ejecutivo Nacional, a causa de las presiones realizadas por empresas y capitales transnacionales interesados en el tráfico y uso ilimitado de los datos de carácter personal. Paradójicamente, el autor del proyecto de la ley había sido el Senador Eduardo Menem, hermano del presidente argentino.

La vetada ley 24.745, seguía los lineamientos de la Ley Orgánica de Regulación del Tratamiento de Datos de Carácter Personal (LORTAD), vigente en

España desde 1992 hasta la promulgación de la Ley Orgánica de Protección de Datos (LOPD) en 1999.

4.2.- Decreto Nacional 1616/96

Como ya adelantamos, la ley 24745 fue totalmente vetada por el Poder Ejecutivo Nacional, a través del Decreto 1616/96, tomando como fundamento:

a) la falta de especificación de las facultades otorgadas a la Comisión Bicameral de seguimiento de la protección legislativa de datos, creada por el artículo 5º de la ley y que por su amplitud vulnera la distribución constitucional de incumbencias estatales;

b) la prohibición del artículo 16 de la ley a la cesión o transmisión de datos entre la República Argentina y otros estados, o con organismos internacionales o supranacionales que no aseguren una protección equivalente de los datos de carácter personal, dado que, según el PEN, esta "disposición ha omitido la previsión de supuestos de excepción en aras de la cooperación internacional y obligaciones asumidas por el Estado Nacional ante otros Estados y organismos". Este argumento cae en el absurdo, puesto que es imposible que por una ley se desconozca un tratado internacional, conforme lo establece el texto del artículo 75 inc. 22 de la Constitución Nacional;

c) la disposición del artículo 35, que permite a los titulares de registros o bancos de datos de titularidad privada, formular códigos tipo para su organización y funcionamiento con recurso ante el Defensor del Pueblo sobre la cual el PEN entiende que "con las previsiones mencionadas se otorgan atribuciones desmedidas a sujetos ajenos a los órganos del Estado, ya que los titulares particulares no pueden crear normas de alcance general que afecten a terceros, por sí mismos, sin sujeción a control posterior alguno por parte de aquellos. Asimismo, se concede al Defensor del Pueblo el ejercicio de funciones jurisdiccionales, en ostensible violación del artículo 86 de la Constitución Nacional, precepto que solo lo legitima

procesalmente para actuar en defensa de los derechos de los ciudadanos". Sobre esta observación, es dable destacar que, con independencia de lo poco clara que aparece la redacción del artículo en cuestión en lo que se refiere a la "formulación de códigos tipo", no surge definitivamente que la atribución asignada al Defensor del Pueblo en la norma en análisis sea una facultad jurisdiccional; d) el mecanismo previsto en el artículo 36 de la Ley en cuanto se regula el procedimiento de la acción de habeas data, "resulta insuficiente para una adecuada tutela del justiciable, sobre todo si se tiene en cuenta que el mismo no es de aplicación contra actos de los entes públicos". Es difícil entender por qué razón el Poder Ejecutivo llega a semejante conclusión, ya que la misma no se desprende de la lectura del artículo en análisis. La observación al artículo 36 continúa refiriéndose a su falta de precisión sobre "cuál será la justicia competente para entender en razón del territorio de la calidad del sujeto demandado, de la afectación del tráfico inter-jurisdiccional o internacional", lo que "genera un vacío susceptible de crear conflictos o interpretaciones divergentes en detrimento de los tutelados por esta ley".

Llama la atención esta observación, especialmente en la medida en que la competencia en razón del territorio, de la calidad de los sujetos demandados y demás situaciones referidas, se rige por la legislación que se ocupa de la competencia de los tribunales, que no se ha pretendido modificar por la ley que analizamos, y tampoco existen fundamentos para que expresamente se establecieran reglas distintas a las habituales en materia de competencia.

En tal sentido debe tenerse en cuenta lo que la propia ley 24745 establecía en su artículo 39, en tanto reconoce la obligatoriedad de que las provincias en sus propios ordenamientos procedimentales contemple las previsiones a efectos de desarrollar la "acción sumarísima para la defensa de los derechos establecidos en la presente ley y en el marco del artículo 43 de la Constitución Nacional", estableciéndose "que la ausencia de reglamentación procesal, no impedirá la tramitación de la acción sumarísima prevista en el artículo 43".

Debiera entenderse, a la vista de esta disposición, que no existe en la ley 24.745 ninguna previsión para alterar la distribución de competencias. De todos modos, es preciso reconocer que la asignación de competencias a la justicia federal o provincial está fijada por los artículos 116 y 117 de la Constitución Nacional.

e) La última observación realizada por el Poder Ejecutivo en orden a proceder al veto de la ley 24.745 se refiere a la atribución de facultades jurisdiccionales punitivas al Defensor del Pueblo, en la medida en que el artículo 38 de la ley lo instituye "como órgano de aplicación de las distintas sanciones que en él se prevén, excediéndose nuevamente en las funciones que le atribuye el artículo 86 de la Carta Magna".

Al respecto, es preciso analizar cuáles son las implicancias de ser órgano de aplicación de una ley, por cuanto aquí radica el centro de la presente observación. En principio, debemos precisar que el legislador tiene facultades constitucionales suficientes para asignar a un órgano creado por el Constituyente, la función de órgano de aplicación de una ley. Siguiendo con este razonamiento, no debe entenderse como asignación de facultades jurisdiccionales punitivas al Defensor del Pueblo, toda vez que se asimila la situación a aquella que se da en el caso de sanciones administrativas que son, como resulta obvio, sin necesidad de que la ley lo establezca, revisables en sede judicial.

El antecedente legislativo inmediato de la ley 25326 fue un proceso complejo que se inicia con posterioridad a la reforma de la Constitución Nacional de 1994, finalizando en su primera etapa con la sanción de la ley 24.745, y el posterior veto total por parte del Poder Ejecutivo Nacional, mediante el decreto 1616/96.

La sanción de la ley 24.745 se realizó sobre la base de la presentación de proyectos de ley tendientes a reglamentar en forma amplia el ejercicio de los derechos tutelados por el habeas data, o incluso de otros proyectos con una intención restringida únicamente a establecer un procedimiento jurisdiccional de ejercicio de la acción de habeas data.

De los proyectos presentados en ambas cámaras, se acordó la aprobación de la ley 24.745, que tuvo como origen a la Cámara de Diputados y a su paso por el Senado de la Nación recibió modificaciones que disgustaron a los diputados nacionales. Por ello, la Cámara de Diputados utilizó la prerrogativa constitucional e insistió con su sanción original, con el voto de los dos tercios de los miembros presentes, dejando al descubierto la diferencia de criterio entre ambas Cámaras del Congreso, independientemente de las pertenencias partidarias de sus integrantes.

Buscando unificar un gran abanico de criterios contradictorios, el Congreso Nacional sancionó un proyecto de ley registrado bajo el número 24.745. El Poder Ejecutivo Nacional lo vetó en su totalidad, mediante el Decreto número 1616/96, publicado el 30 de diciembre de 1996. Si bien no contiene mención alguna en los considerandos, el veto se debió a la presión ejercida por las entidades financieras y las agencias de reportes de créditos.

En la vetada ley 24745 existía una gran influencia de la LORTAD española de 1992 (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal) y una técnica reglamentaria con intención de regulación amplia. Establecía una subespecie de amparo que abarca tanto aspectos de procedimiento de la acción de habeas data, como el control sobre los bancos de datos, las obligaciones de sus titulares y las sanciones administrativas para el caso de que no fueran respetadas.

Siguiendo el método de la LORTAD, comienza determinando su objeto, en la protección de los datos personales tanto de las personas físicas como jurídicas procesados por bancos de datos tanto de carácter públicos como privados.

La ley 24745 expresaba pomposos principios y declaraciones, que luego quedaban vacías de contenido por un abundante sistema de excepciones. Así, comienza enunciando en su artículo 1º, que su objeto es la salvaguarda de los datos personales, tanto de las personas físicas como jurídicas tratados por los registros o bancos de datos públicos o privados. Este mismo artículo precisa que su objeto son

los datos existentes tanto en registros o bancos de datos automatizados como aquellos registrados en soporte físico.

Los principios generales para la protección de datos se encuentran en el Título II, sobresaliendo los siguientes: a) la prohibición de usar datos personales para finalidades distintas de aquellas para las que fueron recogidos y la obligación de ser eliminados cuando hayan dejado de ser necesarios para estos fines; b) la creación de una Comisión legislativa Bicameral de Protección de datos que tenga por objeto posibilitar la salvaguarda y protección de los derechos tutelados en la ley, c) la exigencia del consentimiento expreso y por escrito del titular de los datos, el que puede ser revocado sin efectos retroactivos. En tal sentido se establece el carácter ilícito del tratamiento de datos cuando no se hubiere presentado ese consentimiento por escrito, d) prohibición de dar tratamiento a los datos que revelen ideología, raza, religión, hábitos personales y comportamiento sexual. Asimismo, se excluyen los datos personales que revelen estado de salud, situación patrimonial y obligaciones tributarias, salvo razones de interés general y cuando lo disponga la ley o exista consentimiento del interesado, e) el deber de secreto para quienes intervengan en el tratamiento de los datos de carácter personal, f) la obligatoriedad de consentimiento previo del interesado para que los datos objeto de tratamiento puedan ser cedidos por un registro o banco de datos, etc.

La creación de la Comisión Bicameral de seguimiento de la protección de los datos de carácter personal (art. 5º) fue uno de los argumentos usados por el Poder Ejecutivo Nacional para vetar esta ley, por entender que vulneraba la distribución constitucional de competencias estatales.

El título IV, dedicado a los derechos de los titulares de los datos personales, consagraba: a) la posibilidad de impugnar las valoraciones basadas exclusivamente en el tratamiento de datos de carácter personal; b) el derecho de toda persona a conocer la existencia de registros o bancos de datos de carácter personal, así como su finalidad y la identidad del responsable; c) el derecho del interesado a solicitar información no solo de carácter personal, sino también acerca de quienes hayan

solicitado información sobre su persona; d) el emplazamiento de cinco días hábiles para que el responsable de registro o banco de datos haga efectivo el derecho de rectificación, actualización o eliminación de los datos personales que correspondan; e) la gratuidad del acceso a los datos, su rectificación, actualización, o eliminación cuando fueran inexactos, incompletos o discriminatorios.

Dentro del título V dedicado a los registros y bancos de datos de la Administración Pública Nacional, se crea el Registro General de Protección de Datos, cuya organización se subordinaba al dictado de un decreto reglamentario de la ley, estaba obligado a tomar nota de todos los registros o bancos de datos y debía funcionar en el ámbito de la Dirección Nacional del Registro Oficial.

El art. 26 limitaba el tratamiento de datos personales sin el consentimiento del interesado por parte de las Fuerzas Armadas y organismos de seguridad e inteligencia, a los supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real y cierto para la defensa nacional. Se establecía que los datos de carácter personal registrados por motivos policiales, deben ser eliminados cuando dejaren de ser necesarios para las averiguaciones que motivaron su tratamiento.

Los bancos de datos de titularidad privada son regulados por el Título VI, el cual establece la obligatoriedad de inscripción en el Registro General de Protección de Datos, creado a estos efectos. Este organismo podía rechazar o no disponer la inscripción del banco de datos que lo solicite, mediante resolución fundada en el incumplimiento del titular del banco de datos de los requisitos exigidos por la ley o cuando se afecten los derechos de los titulares de los datos personales almacenados.

Dentro de este título se regula la prestación de servicios sobre información de solvencia patrimonial y crédito, siendo los siguientes aspectos, los más destacados: a) solamente autoriza a tratar datos de carácter personal obtenidos de fuentes accesibles al público o del propio interesado, así como los datos relativos al cumplimiento o no de obligaciones facilitados por el acreedor, estableciéndose que

en todos los casos se notificará al afectado respecto del tratamiento de dichos datos y del registro o banco de datos donde consten los mismos; b) el responsable del registro o banco de datos deberá comunicar en un plazo máximo de cinco días al interesado, cuando este lo solicitara, los datos, evaluaciones o apreciaciones que sobre el mismo hubieran sido elaboradas; e) solamente permitía el tratamiento de datos de carácter personal determinantes para apreciar y evaluar la solvencia y crédito de su titular que no tengan una antigüedad mayor de cinco años.

El artículo 36 de la ley regula el procedimiento de habeas data como una especie de amparo, de trámite sumarísimo y en el cual la sentencia que haga lugar al mismo, mandará la rectificación, actualización o eliminación de los datos de carácter personal, junto a la indemnización por los daños y perjuicios causados.

Conforme lo establecido tanto por el artículo 43 de la Constitución Nacional sobre el amparo, como por el artículo 22 inc. 2 de la ley 24745, no correspondía entender que es obligatorio agotar alguna instancia administrativa con anterioridad a la iniciación de una acción de habeas data.

La posibilidad de aplicar sanciones a los responsables de los registros o bancos de datos que infrinjan la ley, estaba tasada por el artículo 38, que permitía aplicar desde el apercibimiento hasta la clausura. El Defensor del Pueblo es idóneo como órgano de aplicación de acuerdo con la reglamentación que al efecto dicte la Comisión Bicameral establecida en el artículo 5º.

La cesión o transmisión internacional de los datos de carácter personal entre la República Argentina y otros Estados u organismos internacionales o supranacionales, queda prohibida cuando ellos no aseguren una protección equivalente.

La ley 24.745 hubiera podido, en general, dar cierta satisfacción y desarrollo al ejercicio de la garantía constitucional introducida en el artículo 43 tercer párrafo de la Constitución Nacional, a través de la reforma de 1994. El veto realizado por

medio del decreto 1616/96 demoró el desarrollo de la garantía constitucional de habeas data.

4.3.- Proceso de formación de la Ley 25.326

La incorporación del *habeas data* a la Constitución Nacional se había concretado en el año 1994 y luego de seis años de discusión parlamentaria y del veto de la ley sobre habeas data Nº 24745 (año 1996), finalmente el Congreso de la Nación sancionó el 30 de octubre del año 2000, la Ley Nacional de Protección de Datos Personales.

Posteriormente, el Poder Ejecutivo Nacional promulgó en forma parcial el proyecto sancionado por el Congreso de la Nación, que se transformó en la Ley Nacional de Protección de los Datos Personales Nº 25.326[473]. La promulgación fue parcial, dado que el Poder Ejecutivo había vetado los artículos que daban autonomía e independencia a la autoridad de aplicación. Recién entonces fue publicada en el Boletín Oficial el 2 de noviembre de 2000, fecha a partir de la cual entró en vigencia. La ley reglamenta la recopilación, procesamiento y difusión de datos personales por empresas privadas, organismos públicos y particulares, con excepción de aquellos datos procesados por las empresas periodísticas.También desarrolla el Instituto del *habeas data*, incorporado a la Constitución Nacional (art. 43 tercer párrafo de la C.N.), conforme se analizó en el punto anterior, y establece un control estatal sobre empresas y organismos públicos que gestionen y procesen información de carácter personal.

[473] Argentina, Ley Nacional 25.326. Esta norma puede ser consultada en el siguiente sitio web: http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/texact.htm (último ingreso el 26/12/2012)

4.4.- Decreto Nacional 1558/2001

En virtud de lo dispuesto por el artículo 45[474] de la ley 25.326, relativo al plazo de ciento ochenta días hábiles desde su promulgación, otorgados por el Congreso Nacional al Poder Ejecutivo Nacional para reglamentar la Ley Nacional de Protección de Datos y establecer el órgano de control. El Decreto Nacional 1558/2001[475] vino cumplir el mandato de ley: aprobó la reglamentación de la ley 25326 y dispuso la conformación del órgano de control creado por ella en el artículo 29[476].

[474] Argentina, Ley 25326, artículo 45: El Poder Ejecutivo Nacional deberá reglamentar la presente ley y establecer el organismo de control dentro de los ciento ochenta días de su promulgación.

[475] Ley 25.326; Decreto reglamentario Nº 1558/2001. El mismo puede consultarse en el siguiente sitio web: http://www.jus.gob.ar/media/33382/Decreto_1558_2001.pdf (último ingreso el 3/3/2012).

[476] Argentina, Ley 25326, Artículo 29: (Órgano de Control).

1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:

a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;

b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;

c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos o programas de tratamiento de datos, a fin de verificar infracciones al cumplimiento de la presente ley;

e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;

f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;

g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;

h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley.

2. (Punto vetado por art. 1° del Decreto N° 995/2000 B.O. 2/11/2000)

3. (Punto vetado por art. 1° del Decreto N° 995/2000 B.O. 2/11/2000)

El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones.

También, por imperio del artículo 46[477] de la ley 25.326, se estableció un plazo dentro del cual los archivos de datos destinados a proporcionar informes existentes al momento de la sanción de dicha Ley, debían inscribirse en el Registro, establecido por el artículo 21, y adecuarse a lo que dispone el régimen establecido en dicha norma.

El artículo 31, inciso 2, de la Ley Nº 25.326 dispone, además, que la reglamentación determinará las condiciones y procedimientos para la aplicación de sanciones, en los términos que dicha norma establece.

Finalmente, el decreto 1558/2001 invitó a las Provincias y a la Ciudad Autónoma de Buenos Aires a adherir a las normas de exclusiva aplicación nacional existentes en la reglamentación, en particular aquellas normas de forma o procedimiento, dado que el derecho de fondo es competencia del Congreso Nacional y no requiere adhesión de las provincias.

El Decreto 1558/2001 reglamentó el artículo 1º, expresando textualmente que: "a los efectos de esta reglamentación quedan comprendidos en el concepto de archivos, registros, bases o banco de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito".

Como se puede observar, la ley extiende el derecho personalísimo a la protección de los datos personales, a las personas ideales o jurídicas. Observamos que esta extensión puede ser peligrosa para el estado de derecho, ya que hacer opaca y oscura la actividad de las personas jurídicas de existencia ideal, va a contrapelo

[477] Argentina, Ley 25326, artículo 46. — (Disposiciones transitorias).
Los archivos, registros, bases o bancos de datos destinados a proporcionar informes, existentes al momento de la sanción de la presente ley, deberán inscribirse en el registro que se habilite conforme a lo dispuesto en el artículo 21 y adecuarse a lo que dispone el presente régimen dentro del plazo que al efecto establezca la reglamentación (por art. 2° del Decreto N° 1558/2001 B.O. 3/12/2001 se establece en ciento ochenta (180) días el plazo previsto en el presente artículo)

con el principio de registración, transparencia, publicidad y legalidad que debe ser exigido a las personas jurídicas de existencia ideal. Ni Chile, ni España extendieron este derecho humano de tercera generación a las personas jurídicas. Tampoco lo hizo la Directiva Europea 95/46/CE, aunque sí dejó abierta la puerta para que los Estados miembros realicen una protección mayor. En este sentido, sí encontramos la extensión del derecho a la protección de los datos de las personas jurídicas en la legislación italiana y portuguesa.

La ley italiana incorpora la tutela del dato personal de la persona jurídica en el art. 1º, de la ley nº 675/1996, en el cual expresa que la ley garantiza también el derecho de las personas jurídicas y de otros entes o asociaciones. Este mismo artículo, en el apartado 2, dedicado a las definiciones, incluye la protección de los datos personales de las personas jurídicas, al definir dato personal (art. 1.2, c) y titular del derecho (art. 1.2, d). En este mismo sentido, la ley portuguesa de protección de datos, en su artículo 3.1.b) también amplia la titularidad del derecho a la protección de sus datos personales a las personas jurídicas, siempre que los ficheros, bases o bancos de datos contengan datos personales.

Cabe recordar que algunos destacados especialistas en el tema, como el profesor español Emilio Suñé Llinás, marcan la contradicción de exigir transparencia a las personas jurídicas por una parte, y por otra, garantizar su derecho a la intimidad, opacando sus operaciones y participaciones societarias. La protección jurídica de los datos de las personas ideales no debe ser equivalente ni similar a los datos de las personas físicas, dado que la personalidad de las personas jurídicas es una ficción, y como tal, deja de ser un derecho humano, fundamento de una prolija y exigente protección jurídica de la intimidad y de los datos de carácter personal.

El último párrafo del art. 1º expresa que “en ningún caso se podrán afectar las fuentes de información periodísticas”. Al respecto, coincidimos con la opinión de los Senadores Eduardo Menem y Augusto Alasino, quienes expresaron en el debate parlamentario que dejar excluidos expresamente de esta norma los medios

periodísticos y las bases de datos que estos dispongan, como establece el proyecto sancionado, es sobreabundante, ya que la protección a las fuentes periodísticas está incluida en la Constitución. El Senador Alasino votó en contra de la excepción.

5.- Ley 25.326 de Protección de Datos Personales

La Ley 25.326 sigue la lógica de determinados principios, según los cuales los registros deben obtener los datos por medios lícitos y usarlos para fines determinados a priori, con el cuidado de mantener la fidelidad de los datos, respetando la prohibición de suministrar datos a terceros cuando no existiera conformidad del interesado o en casos que encuadren en excepciones especiales.

La ley adopta el principio de prohibición de recoger información "sensible", estableciendo en estos casos una responsabilidad objetiva de los registros si se causara un daño al titular de los datos; por ejemplo, su divulgación ilícita. Intentó poner límites a la actividad de empresas dedicadas a recoger información y datos de las personas.

Pero, quizás el aporte más importante de esta ley es la creación de un órgano de control estatal que tiene como misión controlar a empresas y organismos públicos que trafican datos personales. Este ente, luego denominado Dirección Nacional de Protección de Datos Personales, lleva un registro de bancos de datos, a los que otorga un permiso habilitante. Las personas pueden denunciar a las empresas que no cumplan con la ley, ni con la Constitución, ante el órgano de control que una vez comprobada la falta o el delito contra la intimidad personal, puede entrar en acción, inhabilitando, suspendiendo, aplicando multas e incluso prohibiendo el funcionamiento de una empresa que registre datos personales.

La ley 25.326 ha recibido una fuerte influencia de la legislación española sobre protección de datos personales. Fue reglamentada en junio de 2001, a través del Decreto Nacional Nº 1558/2001. Estas normas establecen que los archivos, registros o bancos de datos públicos y privados destinados a dar información, deben

cumplir reglas y principios. La ley 25.326 de protección de los datos de carácter personal abandonael proceso del juicio de amparo usado por decisión jurisprudencial hasta su entrada en vigencia y crea una nueva vía procesal. Desde el punto de vista procesal, la ley crea un proceso autónomo, diferente y singular.

La ley 25.326 no solo vino a desarrollar la garantía constitucional prevista en el art. 43 tercer párrafo de laConstitución Nacional, sino que también avanza positivamente al crear un marco regulatorio del tratamiento de la información por parte de personas públicas y privadas; establece normas limitativas de la creación de bancos de datos y de la difusión de información pública.

Con relación al control, la ley toma como referencia al sistema europeo, y creauna autoridad de aplicación que el Poder Ejecutivo implementó en el año 2002 con la denominación de Dirección Nacional de Protección de Datos Personales[478], con la misión de velar por el cumplimiento de la normativa sobre protección de datos de carácter personal. Sin embargo, aquí se encuentra el punto más crítico del veto parcial realizado por el Poder Ejecutivo Nacional, a cargo del Presidente De la Rúa en ese momento, dado que privó a esta institución fundamental del sistema de protección jurídica de los datos personales, de autonomía e independencia.

Volviendo al texto de la ley 25.326, luego de manifestar en el artículo 1º una ambiciosa protección jurídica de los datos de carácter personal, realiza en el artículo 2º la descripción de un catálogo de definiciones, imitando el modelo de una técnica legislativa europea, según la cual se describe un catálogo de conceptos y definiciones, que tienden a circunscribir cuál habrá de ser el alcance que se dará a cada término. De estos conceptos, se destaca el de "datos de carácter personal", definido como "cualquier información concerniente a personas físicas o jurídicas, identificadas o identificables sobre características propias o informaciones objetivas".

[478] Dirección Nacional de Protección de datos Personales (autoridad de control de protección de datos personales, Argentina). Fci.: http://www.jus.gob.ar/datos-personales.aspx (último ingreso el 26/12/2012).

Antes de la entrada en vigencia de la ley 25.326, los sucesores de una persona registrada no tenían legitimación activa para acceder a los datos del causante que obren en un banco o base de datos. Una parte de la doctrina sostenía que la muerte, al extinguir la persona -sujeto y soporte de todo derecho- extingue igualmente aquellos bienes jurídicos que le son sustancialmente inherentes. Sin embargo, la sentencia de la Corte Suprema de Justicia de la Nación en el caso Urteaga, ya comentada en este capítulo, había dejado un precedente diferente en la jurisprudencia nacional, que el legislador tomó en cuenta.

La interpretación realizada por la Suprema Corte de Justicia en el caso Urteaga, rompió con la concepción de derecho personalísimo atribuida en forma unánime a la protección de los datos de carácter personal en la doctrina y jurisprudencia internacional. Este antecedente jurisprudencial, junto a la dolorosa historia argentina de miles de personas desaparecidas por motivos políticos en la década de 1970, gravitaron en la discusión y sanción de la ley 25.326 sobre protección de los datos personales, para otorgar legitimación activa a los familiares del titular de los datos.

Hay autores que entienden que en la medida en que se vea afectada esa "intimidad familiar", cabe aceptar el habeas data ejercido para corregir información falsa o discriminatoria sobre el causante, existente en un registro o banco de datos.

Mucho más complejo se torna establecer la legitimación pasiva, ya que el art. 43 menciona a los datos que consten en "registros o bancos de datos públicos, o los privados destinados a proveer informes".

En la jurisprudencia provincial de la Provincia de Tucumán (Argentina), más de un banco de datos se opuso a las acciones de habeas data, aduciendo que su base de datos no está destinada a prestar informes.

Como ya mencionamos, respecto de los registros privados, el art. 43 CN tiene un carácter impreciso limitativo pues se extiende sólo a aquellos "destinados a proveer informes". La norma apunta a incluir en esta categoría principalmente a las

empresas dedicadas a proveer información sobre la capacidad crediticia tanto de personas individuales como colectivas, que generalmente prestan sus servicios a bancos, organizaciones financieras y compañías de seguro. Pero el término "proveer informes" genera un marco de dudas por su imprecisión.

Sólo queda claro que la prensa, ya sea escrita, televisiva u oral, aun cuando tiene por finalidad informar o proveer datos, se encuentra excluida de la legitimación pasiva en la acción de habeas data cuando su objeto es obtener la identidad de los informantes y de sus fuentes de información. El propio constituyente las excluye en forma expresa en la parte final del tercer párrafo del artículo 43 de la Constitución Nacional.

En el caso de los bancos y entidades financieras se observa claramente el problema, dado que su finalidad no es proveer informes, pero las circulares del banco Central establecen que estos suministren determinada información. Estas contradicciones fueron la causa de una jurisprudencia contradictoria, dado que la información financiera es información destinada a divulgarse por disposición expresa de las comunicaciones del Banco Central. Antes de la vigencia de la ley 25.326 y su decreto reglamentario, esta cuestión cobró una importante relevancia, ya que constituía a los Bancos y entidades financieras en sujetos pasivos de la acción de *habeas data*, pues sus registros están destinados a dar información, tal cual lo prevé el art. 43 de la Constitución Nacional. Este problema fue corregido por la jurisprudencia que en la actualidad interpreta que todo banco de datos que puede ser consultado por terceras personas, incluso por empleados del responsable de la base de datos, es un banco de datos destinado a proveer informes.

La garantía constitucional que contiene la acción de habeas data, no solo se dirige a conocer los datos referidos a cada persona, sino también permite obtener la modificación de los datos falsos o de los que importen discriminación o se encuentren desactualizados. Habilita también a exigir la supresión y rectificación o actualización de los datos que así lo requieran y a obtener el carácter confidencial para los datos que deban mantener ese estatus por decisión de su titular. El

accionante se encuentra legitimado para exigir la actualización de sus datos personales.

La norma bajo examen permite a las empresas de marketing recopilar información, pero solo de acceso público, les impide recoger o revelar datos sensibles, datos que de ser revelados, puedan motivar algún tipo de discriminación por razones de raza, orientación sexual, ideas políticas, cuestiones de salud registradas en historias clínicas, identificación con una religión o una actividad gremial.

La norma exige que los archivos, registros o bancos de datos notifiquen por escrito a cada persona que sea incluida en ellos. Se exceptúa de esta obligación a las empresas, que recaban información de listados públicos. Los datos son públicos cuando están incorporados a fuentes de información de acceso público, por ejemplo, la guía de teléfono o el padrón electoral.

5.1.- Objeto de la ley 25.326

El objeto establecido por la ley en el artículo 1°[479] es la protección integral de los datos de personas físicas o de existencia ideal, asentados en bancos de datos u otros medios técnicos de tratamientos de datos, sean estos públicos o privados, destinados a dar informes. El mismo artículo agrega que la ley busca garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre. El último párrafo del artículo ordena que en ningún caso se puedan afectar las bases de datos ni las fuentes de información periodísticas. Con respecto a esta protección especial otorgada por la ley a las bases de datos o fuentes de información periodística, coincidimos con la

[479] Argentina. Ley 25.326. Art. 1º "(Objeto). La presente ley tiene por objeto la protección integral de los datos personales, asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamientos de datos, sean estos públicos o privados, destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, como también el acceso a la información que sobre las mismas se registre, de conformidad con lo establecido en el artículo 43 párrafo tercero de la Constitución Nacional. Las disposiciones de la presente ley también serán aplicables en cuanto resulte pertinente, a los datos relativos a las personas de existencia ideal. En ningún caso se podrán afectar las fuentes de información periodísticas".

opinión vertida por los Senadores Eduardo Menem y Augusto Alasino[480], en el debate parlamentario de sanción de la ley de protección de los datos personales. Los senadores mencionados expresaron que dejar excluidos expresamente de esta norma los medios periodísticos y las bases de datos que estos dispongan, como establece el proyecto sancionado, es sobreabundante, ya que la protección a las fuentes periodísticas está incluida en la Constitución.

El agregado del secreto de las fuentes de información en la parte final del tercer párrafo del art. 43 demuestra que solo se lo incluyó como una excepción al instituto que estudiamos. Por ejemplo, cualquier periodista que sea llamado como testigo, carga con la obligación de testimoniar lo que percibió a través de sus sentidos. El Código Procesal penal no tiene una excepción expresa a estos sujetos, por ello, la interpretación literal del art. 43 conduce a admitir el ejercicio de un derecho de acceso contra los registros de los medios de prensa, pues están destinados a "proveer informes". El límite estará dado por la imposibilidad de conocer el origen de sus fuentes.

Distinto sería considerar a los bancos de datos periodísticos como una excepción al derecho de acceso que establece el habeas data. Sí puede suceder que se intente corregir el dato erróneo o falso no solamente en el banco de datos sino también en su fuente o en las fuentes de donde haya provenido el dato. En este caso, se deberá buscar la fuente o la cadena de transmisión de datos y entonces sí podría verse afectado el secreto de la fuente de información periodística. Se planteará entonces un conflicto entre intimidad y libertad de prensa, que en definitiva deberá ser resuelto judicialmente.

5.2.- Datos personales y otros conceptos

El capítulo I de la ley 25.326 también se ocupa, en su art. 2º, de expresar lo que la ley entiende por datos personales, datos sensibles, archivo, registro, base o banco de datos, tratamiento de datos, responsable del archivo, datos informatizados,

[480] El Senador Augusto Alasino votó en contra de esta excepción.

titular de los datos, usuario de los datos y disociación de los datos. Este artículo no fue reglamentado por el Decreto Nº 1558/2001.

Para la ley 25.326, los datos personales son información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables. Dentro de esta especie, el artículo 2º también define una subespecie a la que llama datos sensibles, a los cuales conceptúa como datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

La ley define indistintamente al concepto archivo, registro, base o banco de datos, como al conjunto de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

La ley considera tratamiento de datos a las operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evacuación, bloqueo, destrucción, y en general el procesamiento de datos personales, como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Para la ley (art. 2º), el responsable de archivo, registro, base o banco de datos es la persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos. Los datos informatizados son, para esta norma, los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado. El titular de los datos es la persona física o de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley. Los usuarios de datos son toda persona pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos. Por último la ley describe el proceso de disociación de datos, como todo

tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

5.3.- Principios de protección de datos

El capítulo II de la ley 25.236 contiene normas relativas a la licitud de poseer un banco de datos, a la calidad y categoría de los datos, al consentimiento del afectado, al deber de informar al titular de los datos, sobre su recolección, la finalidad de la misma y a los derechos que posee como titular de los datos recogidos.

5.3.1.- Licitud de la formación de archivos de datos

El artículo 3º sigue el principio general de licitud de la formación de archivos de datos cuando se encuentren debidamente inscriptos y observen en su operación los principios establecidos por la ley y su reglamentación. Es necesario que no tengan finalidades contrarias a las leyes en general o a la moral pública.

5.3.2.- Prohibición de acumulación de datos sensibles

La categoría de los datos es determinada por el artículo 7º de la ley. Esta norma establece que ninguna persona puede ser obligada a proporcionar datos sensibles. La ley autoriza sólo por excepción a recolectar y tratar datos sensibles cuando existan situaciones de interés general, o cuando sea con finalidades estadísticas o científicas que no permitan la identificación de los titulares de los datos.

La ley distingue entre datos comunes y sensibles (los que revelan orientación sexual, simpatías políticas, sindicales o ideológicas), y prohíbe la recopilación de estos últimos, porque contienen información que revela orientación sexual, preferencias políticas, gremiales, ideológicas y hasta religiosas. Sin embargo, el apartado 3º del artículo 7° exceptúa de esta prohibición a los registros que la Iglesia

Católica, las asociaciones religiosas, las organizaciones políticas y los sindicatos lleven de sus miembros.

Los datos relativos a antecedentes penales y contravencionales solo pueden ser tratados por las autoridades públicas competentes, en el marco de las leyes y de las reglamentaciones respectivas[481].

Sobre los datos relativos a la salud, el artículo 8º permite que los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud, traten datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos y hubieren estado bajo tratamiento de aquellos, siempre que se respeten los principios del secreto profesional.

5.3.3.- Prohibición de bancos de datos que no reúnan condiciones de seguridad

La ley prohíbe registrar datos personales en bancos de datos que no reúnan las condiciones técnicas de integridad y seguridad. El responsable o usuario del archivo de datos tiene la obligación de adoptar las medidas técnicas u organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales. Tales medidas deben ser útiles para detectar desviaciones de información, intencionales o no, por acciones humanas o fallas en el medio técnico utilizado. El objetivo es evitar la adulteración, pérdida, consulta o tratamiento no autorizado de datos personales[482].

5.3.4.- Principio de confidencialidad

El responsable del banco de datos y de las personas que intervengan en cualquier fase del tratamiento de los datos personales, están obligados a cumplir con el deber de confidencialidad y de secreto profesional respecto de los mismos. Esta obligación recae sobre los dependientes, aun después de finalizada su relación con

[481] Argentina. Ley 25.326. Artículo 7º, inciso 4º.
[482] Argentina. Ley 25.326. Artículo 9º (Seguridad de los Datos).

el titular del archivo de datos. El artículo 10 de la ley permite que estas personas puedan ser relevadas de este deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

La ley 25.326 establece como un principio general (Capítulo II), la confidencialidad de la información. Obliga al responsable y a las personas que intervengan en cualquier fase del tratamiento de datos personales, a cumplir con el deber de secreto profesional sobre los mismos. Esta obligación legal opera durante el tratamiento de los datos personales, y aún después de finalizada la relación entre las personas que intervengan en el tratamiento de datos y el titular del archivo de datos[483].

Pero la confidencialidad de la información como principio general sufre las siguientes excepciones establecidas por la ley:

a) Los registros, archivos, o bancos de datos privados no pueden alegar la confidencialidad de la información que requiera un juez, sobre la información concerniente al accionante, en el marco de un proceso judicial sobre protección de datos personales, salvo en el caso de que se afecten las fuentes de información periodística[484].

b) El archivo, registro o banco de datos público se puede oponer a la remisión del informe solicitado en base al artículo 39 de la ley 25.326, invocando las excepciones al derecho de acceso, rectificación o supresión autorizadas por la ley 25.326 o por una ley específica. En estos casos, la ley exige que el banco de datos público acredite los extremos que hacen aplicable la excepción legal. Y si el registro público cumple con tal

[483] Argentina. Ley 25.326; inciso 1º del artículo 10.
[484] Argentina. Ley 25.326; artículos 39 inciso 1º y 40 inciso 1º.

demostración, el juez podrá tomar conocimiento personal y directo de los datos solicitados, asegurando el mantenimiento de su confidencialidad[485].

5.3.5.- Principio de Buena Fe

Este principio aparece junto al lógico objetivo de la Ley 25.326 de proteger los datos personales. Es coherente exigir, salvo contadas excepciones, el consentimiento del titular del dato para la cesión. Este consentimiento es revocable, dado que estamos ante un derecho personalísimo y por ello su titular puede cambiar su voluntad sobre la disposición de sus datos en cualquier momento.

El consentimiento del titular de los datos de carácter personal es constantemente exigido como una obligación legal de los responsables y usuarios de archivos, registros, bases o bancos de datos. La ley considera ilícito el tratamiento de datos personales que no cuente con el consentimiento libre, expreso e informado del titular de los datos. El artículo 5º requiere, en forma expresa, que el consentimiento del titular de los datos conste por escrito o por otro medio que de acuerdo a las circunstancias resulte equiparable. Si el consentimiento es prestado junto a otras declaraciones, debe figurar en forma expresa y destacada, previa notificación al titular de los datos de la información exigida por la ley para que el consentimiento se considere informado. La obligación legal de contar con el consentimiento informado exige a los responsables y usuarios de bancos de datos, que brinden al titular de los datos la información suficiente que le permita evaluar los peligros a los que se expone en caso de consentir el tratamiento o la cesión de sus datos personales.

El artículo 6º de la ley argentina determina, en forma taxativa, que el titular de los datos debe contar con la siguiente información, antes de prestar un consentimiento que se considere libre, expreso e informado: a) la finalidad para la que serán tratados sus datos personales y quienes pueden ser destinatarios de los mismos, o a qué clase de destinatarios pueden ser enviados; b) la existencia del

[485] Argentina. Ley 25.326; artículo 40 inciso 2º.

archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio del responsable; c) el carácter obligatorio o facultativo de las respuestas al cuestionario que se le imponga, en especial cuando se trate de datos sensibles; d) las consecuencias de proporcionar los datos, de la negativa de hacerlo o de la inexactitud de los mismos; e) la posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

5.4.- Cesión de Datos Personales

La cesión de datos personales objeto de tratamiento sólo se encuentra autorizada para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario, siempre que medie el previo consentimiento del titular de los datos.

El artículo 11 de la ley 25.326 exige que se informe al titular de los datos sobre la finalidad de la cesión de sus datos, y que se identifique al cesionario o se informen los elementos que permitan identificarlo. En este caso la coincidencia o la influencia han permitido que la Cesión de Datos aparezca regulada por la LOPD (Ley española vigente) al igual que en la ley argentina, también en el art. 11. En el comentario a esa norma, Mercedes Serrano Pérez expresa que la cesión de datos obliga al responsable del archivo a observar las reglas bajo las cuales la ley permite la comunicación, es decir, el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario y de la recolección previa del consentimiento del interesado para proceder a la misma[486]

5.5.- Obligaciones del cesionario

Las mismas obligaciones legales y reglamentarias, a las que está sujeto el responsable del banco de datos que cede los datos personales, también pesan sobre el cesionario. Ambos, cedente y cesionario, responden solidaria y conjuntamente por la observancia de las obligaciones que le imponen la ley y los reglamentos, ante

[486] Rebollo Delgado, L.; Serrano Pérez, M. (2008). Op. cit., p. 241.

el organismo de control y el titular de los datos personales. El cesionario ocupa el lugar del cedente y es responsable del cumplimiento de las obligaciones legales y reglamentarias en el tratamiento del dato personal; sin embargo, esto no significa que el cedente quede liberado de responsabilidad, dado que concurre solidariamente ante la Dirección de Protección de Datos y ante el titular del dato, sin perjuicio del derecho de repetición que opera en las dos direcciones[487].

El inciso 2º del artículo 11º estatuye que el consentimiento para la cesión de datos es revocable. Ya expresamos que estamos ante una facultad del titular de los datos, que se relaciona directamente con la naturaleza de derecho personalísimo que la doctrina y la jurisprudencia otorgan a los derechos a la intimidad y a la identidad, fundamentos directos del derecho humano de tercera generación a la protección de los datos personales.

Si el responsable o usuario del banco de datos ha cedido datos que luego deben ser rectificados, actualizados o suprimidos, el artículo 16 ordena que se notifique al titular de los datos dentro del quinto día hábil de efectuado el tratamiento de los datos.

Luego de determinar un estatuto de deberes y obligaciones exigidas a los responsables, usuarios, cedentes y cesionarios de datos personales, la ley determina un catálogo de excepciones:

> 1. El tratamiento de datos personales no requiere el consentimiento de su titular cuando[488]: a) los datos se obtengan de fuentes de acceso público irrestricto. b) se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. c) Se trate de listados cuyos datos se limiten al nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio. d) deriven de una relación contractual, científica o profesional del titular de los datos y resulten necesarios para su desarrollo o cumplimiento. e) se trate de

[487] Uicich, R. (2001). Op. cit., p. 81.
[488] Argentina. Ley 25.326; artículo 5º, inciso 2º.

las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes[489].

2. El consentimiento del titular de los datos no es exigido por la ley para la cesión de datos cuando: a) así lo disponga la ley; b) en los supuestos previstos como excepciones a la exigencia de consentimiento del titular de los datos para su tratamiento (artículo 5º inciso 2º); c) cuando se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; d) cuando se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia, o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos, mediante mecanismos de disociación adecuados; e) se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.

5.6.- Transferencia internacional de datos

La ley 25326 prohíbe la transferencia internacional de datos personales, de cualquier tipo, con destino a países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados. El artículo 12º, en su apartado segundo enuncia como excepciones a esta prohibición, los siguientes supuestos de la legislación argentina: a) colaboración judicial internacional, b) intercambio de datos de información médica, cuando lo exija el tratamiento del paciente afectado o una investigación epidemiológica en la cual se hubieran aplicado procedimientos de disociación de la información que hagan inidentificables a los titulares de los datos. c) información relativa a transacciones y transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable, d) cuando la transferencia de datos se hubiera acordado en el marco de

[489] El artículo 5º, inciso 2º, apartado e) precisa que debe tratarse de las informaciones que las entidades financieras reciban de sus clientes conforme a las disposiciones del artículo 39 de la ley 21.526 (ver también el art. 40 de la ley 25.326 y ver la ley 24.144).

tratados internacionales en los cuales la República Argentina sea parte; y e) cuando la transferencia de datos tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

5.7.- Derechos de los titulares de los datos

El capítulo III de la ley 25.326 otorga al titular de los datos, los siguientes derechos sobre sus datos personales: a) el derecho a la información sobre sus datos personales[490]; b) el derecho al acceso a los datos personales[491] c) el derecho a conocer el contenido de la información[492]. d) el derecho de rectificación de sus datos personales[493] e) el derecho de actualización de sus datos personales[494] y f) el derecho a la supresión de sus datos personales[495] g) derecho a impugnar las valoraciones personales fundamentadas en el resultado de un tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado[496]; h) derecho a la gratuidad del ejercicio a la rectificación, actualización y supresión de datos personales.

5.7.1.- Derecho a la información

El titular de los datos tiene el derecho a solicitar al organismo de control toda la información relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables.

[490] Argentina: Ley 25.326; art. 13°.
[491] Argentina: Ley 25.326; art. 14°.
[492] Argentina: Ley 25.326; art. 15°.
[493] Argentina: Ley 25.326; art. 16°.
[494] Argentina: Ley 25.326; art. 16°.
[495] Argentina: Ley 25.326; art. 16°.
[496] Argentina: Ley 25.326; art. 20°.

5.7.2.- Derecho de acceso

El titular de los datos tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos o privados destinados a proveer informes. El artículo 14 de la ley exige al titular de los datos que acredite su identidad, antes de formalizar la solicitud. Cumplido este requisito previo, el responsable o usuario debe proporcionar la información solicitada dentro de los 10 días corridos de haber sido intimado fehacientemente. Si no se satisface esta solicitud en el plazo mencionado, o si el informe no es considerado suficiente por el titular de los datos, queda abierta la vía judicial para plantear la acción de protección de datos personales o habeas data prevista por la ley y la Constitución Nacional.

El responsable del banco de datos no puede exigir pago ni contraprestación alguna al titular de los datos para responder a su solicitud de acceso a sus datos personales, salvo que pretenda ejercer en intervalos menores a los seis meses, sin acreditar un interés legítimo al efecto.

Los sucesores universales pueden ejercer el derecho de acceso cuando el causante titular de los datos personales objeto de la petición de acceso, hubiera fallecido.

5.7.3.- Derecho a conocer el contenido de la información

El titular de los datos tiene el derecho a conocer el contenido de la información que sobre él se encuentra almacenada en el banco de datos. Para garantizar este derecho, el artículo 15, inciso 1º de la ley 25.326 ordena al banco de datos que suministre al titular de los datos la información solicitada, en forma clara, exenta de codificaciones y en su caso acompañada de una explicación de los términos que se utilicen. La explicación exigida no puede revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado. El contenido de la información debe versar sobre la totalidad del registro perteneciente al titular, aun

cuando el requerimiento solo comprenda un aspecto de los datos personales. El informe debe ser amplio y por escrito en un lenguaje accesible a personas que posean una instrucción equivalente al conocimiento medio de la población. La forma en que el banco de datos entrega el informe solicitado está sujeta a la opción que realice el titular de los dados; puede optar por la forma escrita o por medios electrónicos, telefónicos, de imagen u otros idóneos a tal fin.

5.7.4.- Derecho de rectificación de datos personales

El derecho a la rectificación de los datos personales propios, al igual que los derechos a la actualización, a la supresión y a la confidencialidad de los datos, son derechos del titular de los datos personales, y una obligación del banco de datos, cuando así corresponda. La ley 25.326, en su artículo 16 inciso 2º, ordena que el responsable o usuario del banco de datos proceda a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en un plazo máximo de 5 (cinco) días hábiles desde que fue recibido el reclamo del titular de los datos, o desde que fue advertido el error o falsedad. El incumplimiento de la obligación establecida por el inciso 2º del artículo 15º habilita la vía judicial, permitiendo que el interesado promueva sin más la acción de protección de datos personales prevista por la ley.

5.7.5.- Derecho de actualización de los datos personales

Toda persona tiene derecho a exigir al responsable del banco de datos, que sus datos personales incluidos en el banco de datos sean actualizados, cuando así corresponda. El plazo para que proceda el responsable del banco de datos a actualizarlos, es de cinco días hábiles desde recibido el reclamo, al igual que en los derechos de rectificación y supresión. El incumplimiento del responsable o usuario del banco de datos, habilita al afectado a iniciar una acción judicial.

5.7.6.- Derecho de supresión de los datos personales

El derecho a la supresión de los datos personales no procede cuando pudiese causar derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos. El inciso 6º del artículo 16, manifiesta que durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá bloquear el archivo o proveer la información consignando que la misma se encuentra sometida a revisión.

Los datos personales pueden ser suprimidos recién después de cumplidos los plazos previstos en las disposiciones aplicables legales o contractuales que hubieren acordado entre el responsable o usuario del banco de datos y el titular de los datos.

5.7.7.- Derecho a impugnar valoraciones personales

El artículo 20 de la ley 25.326 otorga a los afectados el derecho a solicitar la nulidad insanable y a impugnar, en procesos judiciales o actos administrativos, las valoraciones personales que estén fundamentadas únicamente en el resultado de un tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.

5.7.8.- Gratuidad en el ejercicio de los derechos del titular

El artículo 19 de la ley 25.326 prohíbe la aplicación de cargos al interesado para ejercer los derechos de rectificación, actualización o supresión de sus datos personales inexactos, incompletos o expuestos indebidamente, que obren en registros públicos o privados.

5.7.9.- Excepciones

El artículo 17 de la ley 25.326 estipula los casos en los cuales los responsables o usuarios de bancos de datos pueden denegar el derecho al acceso, a la rectificación o supresión de datos, mediante disposición fundada y notificada al

afectado. Los motivos contemplados por la ley son los siguientes: a) La protección y defensa de la Nación, el orden y la seguridad pública o de la protección de los derechos e intereses de terceros. b) Cuando pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas.

El artículo 17 inciso 3º expresa que las excepciones mencionadas (incisos 2º y 3º) no son oponibles para negar el acceso a los registros, cuando el afectado tenga que ejercer su derecho de defensa.

6.- Comisiones legislativas

Las comisiones legislativas de Defensa Nacional y la Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación, junto a la Comisión de Seguridad Interior de la Cámara de Diputados de la Nación, o aquellas que en el futuro puedan sustituirlas, tienen acceso a los archivos o bancos de datos que traten datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia (artículo 23 inciso 2º).

El art. 18 de la ley 25.326 establece un control parlamentario de los bancos de datos relativos a la inteligencia nacional y fuerzas de seguridad, que coincide con la fiscalización contemplada por la ley de inteligencia Nº 25.520[497].

La ley de Inteligencia creó una Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia, con la intención de fiscalizar para garantizar el cumplimiento de la Constitución y normas dictadas en consecuencia. Por este motivo, esta Comisión tiene amplias facultades para controlar e investigar

[497] República Argentina: Ley Nacional 25.520, publicada en el Boletín Oficial del día 5/12/2001. Ver artículos: 13 inc. f; 15 y 31.

de oficio, y en tal sentido, los organismos del Sistema de Inteligencia Nacional deben suministrar la información o documentación que la Comisión les solicite[498].

7.- Usuarios y responsables de archivos, registros y bancos de datos

El capítulo IV de la ley 25.326 regula el funcionamiento de los bancos de datos junto con las obligaciones de los responsables y usuarios de los mismos.

A excepción de los archivos, registros o bancos de datos de exclusivo uso personal de los particulares, todo otro archivo, registro, base o banco de datos, público o privado destinado a proporcionar informes, tiene la obligación de realizar su inscripción en el registro de la Dirección Nacional de Protección de Datos Personales. La ley prohíbe que los usuarios de datos posean datos personales de naturaleza distinta a los declarados en el registro y ordena que la autoridad de control aplique sanciones administrativas a quienes incumplan estos requisitos.

El artículo 21º en su inciso 2º[499] determina la información mínima que debe comprender el registro de archivos de datos de la Dirección Nacional de Protección de Datos Personales.

Los archivos o bancos de datos pertenecientes a organismos públicos no necesitan que el titular de los datos exprese consentimiento para el tratamiento de sus datos cuando estos sean recabados para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. Esta excepción, que se encuentra reglada en el apartado b) del inciso 2º del artículo 5º de la ley 25.326, no

[498] Palazzi, P. *La Protección de los Datos Personales en Argentina*. Ed. Errepar, Buenos Aires; 2004; pp. 144-145.

[499] Argentina. Artículo 21 inciso 2º: "El registro de archivo de datos debe comprender como mínimo la siguiente información: a) Nombre y apellido del responsable; b)Características y finalidades del archivo; c) Naturaleza de los datos personales contenidos en cada archivo; d) forma de recolección y actualización de datos; e)Destino de los datos y personas físicas de existencia ideal a las que pueden ser transmitidos; f) Modo de interrelacionar la información registrada; g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; h) Tiempo de conservación de los datos; i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de datos."

autoriza a los bancos de datos de organismos públicos a cederlos a usuarios privados de datos sin autorización del titular de los datos.

Los organismos de seguridad e inteligencia tienen un tratamiento especial y pueden recopilar datos personales. Las personas pueden solicitar acceder a la información que se dispone sobre ella, derecho que solo puede ser negado por razones de seguridad nacional. Si esto ocurre, la persona puede recurrir a la justicia para que un juez evalúe los fundamentos expresados por el organismo.

Los bancos de datos pertenecientes a organismos públicos sólo pueden crearse, modificarse o suprimir archivos por medio de disposiciones generales publicadas en el Boletín Oficial de la Nación o diario un oficial. La norma de creación, modificación o supresión del banco de datos de un organismo público debe indicar la siguiente información: a) Las características y finalidad del archivo. b) Las personas respecto de la cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquellas. c) El procedimiento de obtención y actualización de los datos. d) La estructura básica del archivo, informatizado o no y la descripción de la naturaleza de los datos personales que contendrá. e) Las cesiones, transferencias o interconexiones previstas. f) Los órganos responsables del archivo, precisando dependencias jerárquicas en su caso. g) Las oficinas ante las cuales se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión.

Las normas que se dicten para suprimir un registro o banco de datos personales del Estado deben establecer el destino de los datos o las medidas que se adopten para su destrucción[500].

Los bancos de datos personales de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia tienen una regulación diferenciada según la finalidad para la cual fueron creados:

[500] Argentina. Artículo 22 inciso 3º de la ley 25.326.

a) El artículo 23, inciso 1º, establece que quedan sujetos a las disposiciones legales de la ley 25.326 los bancos de datos personales de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia creados para fines administrativos y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran, en virtud de disposiciones legales.

b) El inciso 2º del artículo 23 de la ley 25.326 determina un régimen especial para los bancos de datos personales de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia creados con fines de defensa nacional o seguridad pública. A estos bancos de datos no se les exige el consentimiento del titular de los datos, siempre que: 1. Resulten necesarios para el estricto cumplimiento de las misiones que legalmente le fueran asignadas en materia de defensa nacional, seguridad pública o represión de los delitos; 2. Estén expresamente establecidos a los fines de la defensa nacional, la seguridad pública o la represión de los delitos; 3. Sean específicos y establecidos al efecto; 4. Se encuentren clasificados por categorías, que indiquen el grado de fiabilidad.

c) Por último, la ley 25.326 en su inciso 3º ordena que los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

8.- Archivos, registros o bancos de datos privados

Todo banco de datos, archivo o registro de datos personales formado por los particulares y que no sean para uso exclusivamente personal tienen la obligación legal de registrarse en el registro habilitado a tal efecto por la Dirección Nacional de Protección de Datos Personales, conforme lo establecen los artículos 21 y 24 de la ley 25.326.

Cuando estos bancos de datos presten servicios de tratamiento de datos personales por cuenta de terceros, no pueden aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni si quiera para su conservación.

Una vez cumplida la prestación contractual, los bancos de datos privados están legalmente obligados a destruir los datos personales que hubieran tratado. Solo se pueden conservar los datos personales con las debidas condiciones de seguridad y por un período de hasta dos años, en los siguientes casos: 1. Cuando medie una autorización expresa de aquel por cuenta de quien se prestan los servicios; 2. Cuando razonablemente se presuma la posibilidad de ulteriores encargos.

El artículo 25º, dedicado a la prestación de servicios informatizados de datos personales, establece en su apartado 1º que el prestador que procese este tipo de datos personales por cuenta de un tercero, no podrá aplicar o utilizar tales datos con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni siquiera para su conservación. El apartado 2º ordena que, una vez cumplida la prestación contractual, los datos personales tratados deben ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios, o cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

9.- Prestación de servicios de información crediticia

El artículo 26 de la ley 25.326 busca establecer pautas de funcionamiento para las empresas que operan en el sector de los servicios de información crediticia.

En este rubro encontramos a los archivos o bancos de datos de información crediticia, cuya actividad consiste en la venta de listados donde aparecen los

antecedentes financieros de las personas. En Argentina, la organización Veraz ha captado la mayor parte del mercado.

La cesión de datos tratados para la prestación de servicios de información crediticia no requiere el previo consentimiento del titular de los datos, ni la ulterior comunicación de ésta, cuando los datos estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios[501].

Las empresas de información crediticia sólo pueden archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico – financiera de las personas afectadas, durante los últimos cinco años. Este plazo se reduce a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho en el registro informático. La ley establece un límite temporal de permanencia de los datos relativos a la prestación de servicios de información crediticia[502].

El apartado 1º del artículo 26 establece que en la prestación de servicios de información crediticia, solo pueden tratarse datos patrimoniales de carácter patrimonial relativos a la solvencia económica y al crédito. La información sólo puede ser obtenida de fuentes accesibles al público o procedente de informaciones facilitadas por el interesado o con su consentimiento.

El apartado 2º agrega que, cuando se trate de datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, esos datos pueden ser facilitados por el acreedor o por quien actúe por su cuenta o interés.

A solicitud del titular de los datos, el responsable o usuario del banco de datos le comunicará las informaciones, evaluaciones y apreciaciones que sobre el

[501] Argentina. Artículo 26, inciso 5º de la ley 25.326.
[502] Argentina. Artículo 26, inciso 4º de la ley 25.326: "Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económica financiera de los afectados durante los últimos 5 años. Dicho plazo se reducirá a 2 años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho".

mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.

10.- Archivos, registros o bancos de datos con fines de publicidad

Los datos que figuran en documentos accesibles al público y aquellos que hayan sido facilitados por los propios titulares, u obtenidos con su consentimiento, pueden ser tratados para establecer perfiles determinados con fines promocionales, comerciales o publicitarios, o que permitan establecer ámbitos de consumo.

En estos bancos de datos, el titular de los datos puede ejercer el derecho de acceso sin cargo alguno, y solicitar el retiro o bloqueo de su nombre de los bancos de datos con fines de publicidad.

11.- Archivos, registros o bancos de datos relativos a encuestas

Cuando los datos recogidos no puedan atribuirse a una persona determinada o determinable, la ley 25.326 de protección de los datos de carácter personal no se aplica a las encuestas de opinión, las mediciones y estadísticas[503], los trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas.

El inciso 2º del artículo 28 de la ley de protección de datos personales ordena que, en caso de imposibilidad de mantener el anonimato durante el proceso de recolección de datos, se debe utilizar una técnica de disociación, de modo que no se permita identificar a persona alguna.

12.- Órgano de control

El Capítulo V, en su artículo 29, crea un órgano de control o autoridad oficial de aplicación dependiente del Ministerio de Justicia, al cual la reglamentación dictada por medio del Decreto 1558/2001, ha denominado Dirección Nacional de

[503] La ley 17.622, legisla sobre las mediciones y estadísticas.

Protección de los Datos Personales[504]. El órgano de control debe realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la ley. Entre sus principales responsabilidades, se encuentra la obligación de llevar un registro de todos los archivos o bancos de datos existentes, a los efectos de determinar quiénes y con qué finalidad acumulan información personal. Su principal función es registrar y controlar a empresas, organismos y particulares que trabajen con bases de datos personales y confidenciales, a quienes puede sancionar con multas, suspensiones e inhabilitaciones, si violan la ley.

Las funciones y atribuciones determinadas por el artículo 29 de la ley 25.326 para el organismo de control, son las siguientes: a) Asistir y asesorar a las personas que lo requieran, acerca de los alcances de la ley, su reglamentación y de los medios legales de que dispongan para la defensa de los derechos que esta garantiza. b) Dictar normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por la ley 25.326. c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos. d) Controlar la observancia de las normas sobre integridad y seguridad de los datos por parte de los archivos, registros o bancos de datos. A tal efecto puede solicitar autorización judicial para acceder a locales, equipos o programas de tratamiento de datos, a fin de verificar infracciones al cumplimiento de la ley 25.326. e) Solicitar información a las entidades públicas o privadas, las que deberán proporcionar antecedentes, documentos, programas u otros documentos relativos al tratamiento de los datos personales que se les requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados. f) Imponer sanciones administrativas que en su caso correspondan por violación a la ley 25.326 y a sus reglamentos. g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la ley de protección de datos de carácter personal. h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados

[504] Dirección Nacional de Protección de los Datos de Carácter Personal (Argentina). Op. cit. Fci.: http://www.jus.gov.ar/minjus/dpdp/.

destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por la ley 25.326.

La ley ordena que el órgano de control lleve un registro de las empresas que procesan datos personales y les otorgue un permiso habilitante cuando cumplan con todos los requisitos exigidos por la ley y su decreto reglamentario. También le corresponde fomentar que los ciudadanos realicen denuncias a las empresas ante el órgano de control. Las denuncias obligan que el órgano de control se ponga en acción, inhabilite, suspenda y aplique multas e incluso prohíba que una empresa siga prestando este servicio.

Los apartados 2º y 3º del artículo 29 del proyecto de la ley 25.326, sancionados por el Congreso de la Nación, diseñaron un órgano de control con autonomía funcional, descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación y dirigido por un Director designado por el término de cuatro años por el Poder Ejecutivo con acuerdo del Senado de la Nación, seleccionado entre personas con antecedentes en la materia. Estos dos apartados (2º y 3º) de la ley 25.326, fueron vetados por el decreto 995/2000 del Poder Ejecutivo de la Nación, y de esta forma se extirpó de la ley una eficaz herramienta de control, cuya función principal era velar por el cumplimiento de la ley, en forma imparcial e independiente de los organismos gubernamentales que forman parte del Poder Ejecutivo de la nación

En cambio, fueron promulgadas las especificaciones que habilitan al Poder Ejecutivo a remover al Director Nacional de Protección de Datos Personales por mal desempeño de sus funciones, debilitando aún más su precaria situación[505].

El artículo 29 de la ley 25.326 fue reglamentado a través del Decreto 1558/2001, a partir del cual se crea la Dirección Nacional de Protección de Datos Personales, en el ámbito de la Secretaría de Justicia y Asuntos Legislativos del

[505] Argentina. Ley 25.326; artículo 29 in fine: "El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones".

Ministerio de Justicia y Derechos Humanos. Esta norma indica que el Director ejercerá sus funciones con plena independencia y no estará sujeto a instrucciones, contando con un Consejo Consultivo *ad honorem*, para su asesoramiento en los asuntos de importancia.

La integración del Consejo Consultivo se realiza con representantes de instituciones públicas y privadas, taxativamente enumeradas por el Decreto 1558/2001.

13.- Códigos de conducta

Los códigos de conducta, definidos por Gozaíni como reglas deontológicas de cada sector comprometido con el tratamiento de datos personales, son principios de que se establecen para las empresas, usuarios y consumidores[506]. Tienen la particularidad de ser elaborados por la propia institución que se va a someter a esas reglas, de modo que funcionan como un sistema de autorregulación.

La autorregulación por medio de códigos de conducta, tiene sus antecedentes en la legislación europea. En España, tanto la ley de protección de datos personales derogada (LORTAD, 1992) como la actual ley en vigencia (LOPD, 1999), fomentan la elaboración de estas normas de autorregulación, a las que denominan código deontológicos tipo[507].

La ley 25.326 establece la posibilidad de que las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada, propongan su autorregulación por medio de códigos de conducta de práctica profesional, estableciendo normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información, en función de los principios establecidos por la ley[508].

[506] Gozaíni, O. (2002). Op. cit., p. 374.
[507] España. LORTAD (Derogada), artículo 31.2. LOPD Nº 15/99 (en vigencia), art. 32.Op. cit.
[508] Argentina. Ley 25.326; art. 30, apartado 1º.

El apartado 2º del artículo 30 de la ley, ordena al órgano de control que lleve un registro de estos códigos de conductas. El Director puede denegar la inscripción de un código, cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia. El Decreto 1558/2001 asigna al Director la función de homologar los códigos de conducta que se presenten. La homologación debe hacerse con un dictamen previo del Consejo Consultivo y considerando su adecuación a los principios reguladores del tratamiento de datos personales, la representatividad que ejerza la asociación y el organismo que elabore el código y su eficacia ejecutiva con relación a los operadores del sector, para lo cual debe prever sanciones o mecanismos adecuados[509].

El Reglamento de la ley decreta que la Dirección Nacional de Protección de Datos Personales alentará la elaboración de Códigos de Conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por la ley de protección de datos personales y su decreto reglamentario. Este decreto 1558/2001 confirma la importancia que le da la ley a los códigos de conducta, al reglamentar este artículo 30 de la ley y destacar que la propia Dirección Nacional de Protección de Datos Personales alentará la elaboración de los códigos de conducta.

Mientras el artículo 30 de la ley 25.326 autoriza que los bancos de datos privados elaboren códigos de conducta a través de sus organizaciones, el Decreto reglamentario amplía esta posibilidad a las entidades representativas de bancos de datos públicos. El legislador argentino ha imitado incluso estas diferencias existentes en España entre la ley derogada (LORTAD) y la ley vigente (LOPD), promulgada en 1999.

El Decreto Reglamentario 1558/01, en el art. 30 ordena a la Dirección de Protección de Datos, alentar la elaboración de códigos de conducta destinados a

[509] Argentina. Decreto Nacional Nº 1558/2001; inc. f) del apartado 5º de la reglamentación del artículo 29 de la ley 25.326.

contribuir en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales.

El legislador pone en poder de las asociaciones y representantes de responsables o usuarios de bancos de datos de titularidad privada, la posibilidad de elaborar códigos de conducta, a efectos de establecer reglas específicas tendientes a normar la actividad de cada sector, atendiendo a las particularidades de cada uno de ellos[510].

14.- Sanciones administrativas y penales

La ley 25.326 establece tanto sanciones administrativas como penales para los responsables o usuarios de bancos de datos que la incumplan[511].

Las sanciones administrativas pueden consistir en apercibimiento, suspensión, multa, clausura o cancelación del archivo, registro o banco de datos, aplicadas por el órgano de control. Además de las responsabilidades administrativas que correspondan a los infractores, puede caber responsabilidad por daños y perjuicios derivados de la inobservancia de la ley 25.236, o bien sanciones penales para conductas determinadas por el Código Penal.

Las sanciones administrativas deben graduarse con relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción[512].

La reglamentación establece las condiciones y procedimientos para la aplicación de las mencionadas sanciones administrativas a los responsables o usuarios de bancos de datos públicos, y privados destinados a dar información. Se considerará reincidente a quien, habiendo sido sancionado por una infracción a la ley 25.326, o sus reglamentaciones, incurriera en otra de similar naturaleza dentro del término de tres (3) años, a contar desde la aplicación de la sanción.

---

[510] Basterra, M. I. (2008). Op. cit., p. 510.
[511] Argentina. Ley 25.326, capítulo VI.
[512] Argentina. Ley 25.326; artículo 31º, apartado 2º.

En materia penal, el artículo 32º de la ley 25.326 incorporó al Código Penal los artículos 117 bis[513] y 157 bis[514] que establecían penas de prisión de un mes a tres años, por violación a las normas de protección de datos personales que establece la ley.

El incumplimiento de la ley por parte de un funcionario público ha sido sancionado con una duplicación de las penas. El legislador busca de esta forma desalentar todo tipo de procesamiento de datos ilícitos dentro de la administración pública.

Posteriormente, el Código Penal argentino fue reformado por la ley 26.388[515] y se derogó parcialmente el art. 117 bis, pasando parte de su tipo penal a acumular los tipos penales del art. 157 bis, que actualmente quedó redactado de la siguiente forma: artículo 157 bis. "Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario

[513] Artículo 117 bis del Código Penal: 1º. Será reprimido con la pena de prisión de un mes a dos años al que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.
2º. La pena será de seis meses a tres años al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.
3º. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.
4º. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena.

[514] Artículo 157 bis del Código Penal: Será reprimido con la pena de prisión de un mes a dos años el que:
1º. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2º. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.
Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años.

[515] *Ley 26388* (Argentina), publicada en el Boletín Oficial el día 25 de Junio de 2008.

público sufrirá, además, pena de inhabilitación especial de uno (1) a cuatro (4) años[516].” (Artículo sustituido por art. 8° de la Ley N° 26.388, B.O. 25/6/2008).

Los motivos de esta reforma al Código Penal del año 2008, en la derogación del inc. 1º del art. 117 bis, tienen que ver con la ubicación originaria de este artículo que se encuentra en el Titulo del “derecho al honor”, por una más conveniente en el Capítulo III, referido a la Violación de Secretos y de la Privacidad.

15.- Etapas del proceso de protección de datos personales

El ejercicio del derecho a la protección de datos personales puede desarrollarse en procedimiento que se tramita dentro de los tribunales o fuera de ellos. Normalmente la primera etapa es extrajudicial y si esa no arriba a un entendimiento o acuerdo entre las partes, se plantea el procedimiento judicial.

15.1.- Etapa extrajudicial

Los derechos garantizados por el tercer párrafo del artículo 43 de la Constitución Nacional referidos a la garantía constitucional de habeas data pueden ejercerse por medio de reclamos extrajudiciales o bien directamente a través de una acción judicial[517].

Los reclamos extrajudiciales se pueden realizar en una etapa prejudical previa a todo planteo judicial. En esta etapa, la persona que se siente agraviada en su intimidad por la acumulación o uso ilícito de sus datos personales, puede notificar fehacientemente al titular del banco de datos, solicitándole la exhibición del registro o dato, y en su caso la corrección de los datos existentes en el asiento informático. El artículo 14 de la ley 25.326 contempla el reclamo extrajudicial para el ejercicio del derecho de acceso. Indica que el titular de los datos puede, previa acreditación de su identidad, solicitar y obtener información de los datos personales incluidos en los bancos de datos públicos o privados destinados a proveer informes.

[516] El inc. 1º del art. 117 bis del Código Penal fue sustituido por el art. 14º de la ley 26388.
[517] Ekmekdjian, M.; Pizzolo Calogero (h). (1996). Op. cit., p. 101.

El banco de datos debe proporcionar la información solicitada dentro de los diez (10) días corridos de haber sido intimado fehacientemente. Vencido el plazo, sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará habilitada la vía judicial para interponer una acción de protección de los datos de carácter personal.

Puede ocurrir que el archivo, banco o base de datos que acumuló la información personal referida, consienta la exhibición del registro y no hubiera ningún dato que rectificar o suprimir. O bien, que una vez exhibido el registro, hubiera datos a corregir, y la parte acumuladora de datos los corrija en forma rápida, dando respuesta al ejercicio del derecho de habeas data en esta etapa prejudicial.

La ley ordena que el derecho de acceso sea ejercido en forma gratuita durante intervalos no inferiores a seis (6) meses. El acceso gratuito también puede ser permitido cuando el afectado lo solicite en un intervalo inferior a los seis meses, acreditando un interés legítimo al efecto.

15.2.- Etapa judicial de protección de datos personales

Se llega a la etapa judicial cuando la persona que recaba, procesa o cede datos personales: 1) se niega a exhibirlos; 2) no responde al solicitante o 3) si exhibiendo el registro, se niega a rectificar o cancelar los datos cuestionados, siendo en el ámbito nacional de aplicación la vía judicial, establecida en el capítulo VII de la ley 25326. La vía judicial exige, para quedar habilitada, una negativa expresa o implícita (silencio) del acumulador de los datos[518].

La vía judicial también queda habilitada cuando el banco de datos hubiera permitido a terceros, el acceso a datos sensibles sin autorización del titular de los datos. En este caso no es necesario cumplir previamente con la reclamación prejudicial[519], ya que la violación al derecho a la intimidad y a la protección de datos personales se consumó de antemano. En estos casos queda habilitada, para el

[518] Ibidem, p. 102.
[519] Ibidem.

titular de los datos, la acción judicial de protección de datos personales establecida en la ley 25326, en la cual también se puede exigir el derecho de réplica en su caso, o una indemnización del daño moral o material fundada en el artículo 1071 bis del Código Civil.

El sujeto pasivo de la relación es la entidad a cuyo resguardo se halla el registro cuestionado. Puede oponer defensas legítimas a la exhibición de los datos, o bien negarse a rectificarlos, suprimirlos o darle carácter confidencial. Si se trata de órganos del Estado, la contestación puede ampararse en razones de defensa nacional o seguridad interior y negar de esta forma el acceso al banco de datos y la modificación de los mismos.

Al igual que en las normas europeas que le sirvieron de antecedentes, la ley argentina[520] autoriza a los responsables o usuarios de bancos de datos públicos a denegar el acceso, rectificación o la supresión de datos personales, mediante resolución notificada al interesado y fundada en las siguientes causas: 1) la protección de la defensa nacional, del orden y la seguridad pública o la protección de los derechos e intereses de terceros; 2) el peligro de obstaculizar actuaciones judiciales o administrativas en curso vinculadas a una investigación sobre el cumplimiento de obligaciones tributarias o previsionales; 3) el desarrollo de funciones de control de la salud y del medio ambiente; 4) la investigación de delitos penales; y 5) la verificación de infracciones administrativas.

Recordemos que el art. 43 tercer párrafo de la Constitución Nacional permite el ejercicio de la acción de habeas data a toda persona afectada, tendiente a permitir que tome conocimiento de los datos a ella referidos y de su finalidad. De este

[520] Argentina. Ley 25.326; artículo 17 (Excepciones): "1. Los responsables o usuarios de bancos de datos públicos pueden mediante decisión fundada denegar el acceso, rectificación o la supresión en función de la protección de la defensa nacional, del orden y la seguridad pública o de la protección de los derechos e intereses de terceros. 2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo, se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculados a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga, deberá ser fundada y notificada al afectado".

precepto constitucional surge que el derecho de acceso a la información asiste a toda persona que desee conocer los datos que contenga un banco, base o archivo de datos sobre su persona. La toma de conocimiento implica el ejercicio del "derecho de acceso a la información", el cual tiene por finalidad permitir al individuo el control sobre la información que le concierne, que es en esencia uno de los objetivos principales del habeas data.

La posibilidad de suprimir, rectificar, actualizar o solicitar la confidencialidad de información que el art. 43 tercer párrafo de la Constitución Nacional y el artículo 33 de la Ley 25.326 otorgan al registrado, constituyen un corolario del derecho a controlar la información. Estos derechos que también componen el habeas data, surgen en caso de comprobarse el error o la falsedad de los datos o cuando aun sin ser falsos tengan por objetivo o finalidad una acción discriminatoria, o bien que los datos se encuentren desactualizados[521].

El artículo 33º[522] de la ley 25326, relativo a la procedencia de la acción de protección de los datos personales, establece que esta acción procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados, destinados a proporcionar informes, y de la finalidad de aquellos; y b) en los casos en que se presuma falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la ley (25.326), para permitir al accionante exigir su rectificación, supresión, confidencialidad o actualización.

El trámite judicial de la acción de protección de datos personales, que persigue el acceso a la información, se encuentra regulado por el artículo 39 de la ley 25.326. Admitida la acción, el juez requiere al archivo, registro o banco de datos la remisión de la información concerniente al accionante. El funcionario judicial

[521] Distinta fue la redacción del *habeas data* legislado por la Ciudad Autónoma de Buenos Aires, programado en una forma mucho más amplia, ya que permite actualizar, rectificar, requerir la confidencialidad o la supresión, "cuando esa información lesione o restrinja algún derecho" (art. 16 del Estatuto Organizativo de la Ciudad de Buenos Aires).
[522] El decreto 1558/2001 no reglamentó los artículos 33 a 46 de la ley 25.326.

también puede solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente.

El demandado cuenta con un plazo de cinco días hábiles para contestar el informe solicitado por el juez. Este plazo puede ser ampliado prudencialmente por el magistrado.

Como puede observarse, el acceso a la información se produce luego de la respuesta por parte del demandado al requerimiento judicial de informe, en el cual el demandado realiza una presentación de los datos solicitados en el expediente judicial.

Una vez que el accionante ha tomado conocimiento del o de los datos requeridos y de su finalidad, deberá probar que existe falsedad o la intención de un uso discriminatorio, para recién poder acceder a una segunda etapa, en la cual se pueden ejercer los otros derechos de rectificación, supresión, confidencialidad o actualización de la información personal.

A los fines del *habeas data* encontramos que la jurisprudencia argentina no ha terminado de elaborar un concepto pacífico de falsedad de datos. Si falso es todo aquello que no está de acuerdo con la realidad, cabe preguntarse, por ejemplo, si un dato incompleto es un dato parcialmente falso, que pueda dar lugar a la acción de *habeas data*. La doctrina también ha sostenido que existen datos desactualizados cuando la información cuestionada no incluye nuevos elementos o hechos importantes que se relacionen con la persona a quien se refieren. En estos casos es posible exigir a través de la acción de protección de datos personales, que el juez ordene la actualización de la información, incluyendo la incorporación de datos que no constaban en los registros o archivos.

En cuanto a sus efectos, también es necesario distinguir la falsedad de la discriminación. La falsedad habilita a peticionar la supresión, rectificación o actualización, pero no la confidencialidad. Ante la discriminación, es posible

solicitar la supresión del dato lesivo, o bien la confidencialidad del mismo. La discriminación puede provenir de un trato que revista tal carácter en función de una información almacenada en una base de datos que contenga una información determinada. Sin embargo, discriminación y falsedad pueden combinarse; así, por ejemplo, sería discriminatorio para una persona, el figurar en una base de datos o fichero que le sindique una determinada creencia religiosa, una idea política, o cualquier otra información de carácter sensible, cuando no reviste tal carácter. Por eso, el trato discriminatorio que sufre el afectado puede corregirse mediante la modificación o supresión del dato.

No se conocen acciones de protección de datos personales basadas en el motivo de la discriminación; en cambio, se basaron en otros motivos, tales como la caducidad del dato por el transcurso del tiempo. En estos casos, los afectados intentaron suprimir los datos que mantenían las agencias de informes comerciales, sosteniendo que los mismos estaban caducos por haber transcurrido un espacio de tiempo excesivo al previsto por la ley.

La supresión busca eliminar el dato falso o discriminatorio, que afecta la verdad o la igualdad. Es posible solicitar la supresión cuando el dato ha entrado erróneamente al registro; la jurisprudencia de los Estados Unidos de América admite que existe un derecho por parte de la persona que fue arrestada sin causa probable de eliminar esos antecedentes penales del registro, o cuando los datos personales ya no sean necesarios para los fines que contemplaron su almacenamiento.

Distinto es el contenido del derecho a la confidencialidad, por el cual se tiende a proteger la intimidad del individuo, aislando sus datos sensibles. Tal sería el caso de preservar la información sobre las enfermedades que figuren en la historia clínica, o de impedir la identificación de un portador de HIV, de acuerdo a lo que establece la ley respectiva. La acción de protección de datos personales también se puede plantear para peticionar la confidencialidad de una declaración jurada que está por ser dada a publicidad, salvo que el requerido sea un medio de

prensa, en cuyo caso la prohibición de censura previa se levanta como una barrera infranqueable para hacer lugar a una medida de tal especie.

A partir del artículo 1º *in fine* de la ley 25.326, es posible usar la acción de protección de datos personales para mantener la confidencialidad de una fuente de información periodística. El artículo mencionado y la Constitución Nacional en el artículo 43 tercer párrafo, otorgan a las empresas periodísticas una excepción al derecho general de acceso y control de la información.

El afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, poseen legitimación activa para accionar por sí o por intermedio de apoderado[523]. Cuando el agravio afecta a una persona ideal, la acción deberá ser interpuesta por sus representantes legales o apoderados que éstas designen al efecto. En este proceso, el Defensor del Pueblo también se encuentra legitimado activamente para intervenir en forma coadyuvante.

Aun cuando la doctrina ha entendido en forma pacífica que el derecho a la protección de datos personales es un derecho personalísimo, la ley 25326 ha legislado a contramano de esta unánime coincidencia internacional, extendiendo este derecho no solo a las personas jurídicas, sino también a los tutores, curadores y sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado por sí o por intermedio de apoderado. La extensión de la legitimación activa en la ley argentina, se encuentra en la propia historia argentina, y en las consecuencias del gobierno militar que ocupó los años 1976 a 1983. Este traumático proceso de la historia argentina dejó una larga lista de personas desaparecidas. La llegada del habeas data a la Constitución Argentina en 1994, se interpretó como una solución para que los familiares de los desaparecidos lograran información sobre ellos. La jurisprudencia hizo lugar a diversos planteos de este tipo[524].

Del artículo 35º, surge que la legitimación pasiva procede respecto de los responsables y usuarios de bancos de datos públicos y de los privados destinados a

[523] Argentina, Ley 25.326; artículo 34.
[524] Caso Urteaga, F. c/ Escuela de Mecánica de la Armada; CSJN. Op. cit.

proveer informes. El artículo 2º de la ley 25.326 define el concepto de responsable del archivo, registro, base o banco de datos, diciendo que es toda persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos. Usuario es toda persona, pública o privada que realice a su arbitrio el tratamiento de banco de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

Para la ley 25.326, el concepto de archivo, registro, base o banco de datos designa indistintamente al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Con respecto a la competencia, nada dice el tercer párrafo del artículo 43 de la Constitución Nacional; por ello, es útil lo normado por el artículo 36º de la ley 25326. El precepto legal mencionado deja a elección del actor, la competencia del juez que va a entender en la acción de protección de datos personales. El actor puede optar entre la competencia que corresponde al juez de su domicilio, la que corresponda al juez del domicilio del demandado o al juez del lugar en el cual el hecho o acto se exteriorice o pudiera tener efecto. El mismo artículo 36º indica que procederá la competencia federal cuando se interponga la acción en contra de archivos de datos públicos de organismos nacionales y cuando los archivos de datos se encuentren interconectados en redes inter-jurisdiccionales, nacionales o internacionales.

El procedimiento aplicable a la acción de protección de datos personales[525], surge de las disposiciones de la propia ley y por el procedimiento que corresponde a la acción de amparo común. Supletoriamente se aplican las normas del Código Procesal Civil y Comercial de la Nación en lo atinente al juicio sumarísimo[526].

La acción de protección de datos personales se inicia con una presentación o demanda, que debe ser interpuesta por escrito, individualizando con precisión el

[525] Argentina. Ley 25.326; artículo 37.
[526] Argentina. Código Procesal Civil y Comercial de la Nación; artículos 229 y 232.

nombre y domicilio del archivo, registro o banco de datos y en su caso el nombre del responsable o usuario del mismo. Si el banco de datos fuera público, se debe intentar establecer el organismo estatal del cual depende[527].

Es posible solicitar medidas cautelares o precautorias, junto con la acción de protección de datos personales. Previamente es necesario cumplir con los requisitos que el Código Procesal Civil y Comercial de la Nación requiere para las medidas cautelares. El peticionante debe cuidar que la medida cautelar y el objeto del proceso -que en el *habeas data* suele ser suprimir, actualizar o rectificar la información-, no coincidan, pues ello llevaría al rechazo de la medida. Puede el actor solicitar que el demandado se abstenga de difundir el dato mientras dure el pleito. El juez tiene la posibilidad de exigir que el responsable del archivo, base o banco de datos, realice una anotación en el registro, por la cual se exprese que los datos expuestos se encuentran cuestionados o sometidos a juicio[528]. Como vemos, el cuestionamiento del dato en un litigio es el fundamento para solicitar la medida cautelar de anotación de litis en el propio registro demandado, con la obligación de informar, al difundir el dato a terceros.

El juez competente en la acción de protección de datos personales puede disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio, cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate[529].

Si el juez admite la acción, debe requerir al archivo, registro o banco de datos, la remisión de la accionante. Podrá solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección, y cualquier aspecto que resulte conducente a la resolución de la causa que estime procedente. El plazo para

[527] Argentina. Ley 25.326; artículo 38.
[528] Argentina. Ley 25.326; inciso 3º del artículo 38.
[529] Argentina. Ley 25.326, inciso 4º del artículo 38.

contestar el informe no puede exceder los cinco días hábiles, plazo que puede ser ampliado prudencialmente por el juez[530].

Al contestar el informe[531], el archivo o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado, de conformidad y en la forma establecida por la ley[532] para el ejercicio del derecho de acceso[533].

Una vez contestado el informe, el actor puede, en el término de tres días, ampliar el objeto de la demanda, solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales. En este mismo acto debe ofrecer prueba que demuestre los motivos por los cuales resulta procedente, en cumplimiento de la ley 25.326, proceder a la supresión, rectificación o exigir la confidencialidad o actualización de los datos personales indicados[534]. El juez dará traslado[535], por tres días, de esta presentación al demandado.

Vencido el plazo para la contestación del informe, o contestado el mismo, o en el supuesto de ampliación de la demanda y contestada la ampliación, habiendo sido producida en su caso la prueba, el juez debe dictar sentencia haciendo lugar a la acción o rechazándola[536], y debe comunicarla al organismo de control que deberá llevar un registro de las mismas.

Si el juez estima procedente la acción, debe especificar si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, y establecer un plazo para su cumplimiento[537]. El rechazo de la acción, por parte del juez, no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante.

---

[530] Argentina. Ley 25.326; artículo 39.
[531] Argentina. Ley 25.326; artículo 41 (Contestación del Informe).
[532] Argentina. Ley 25.326; artículo 15.
[533] Argentina. Ley 25.326; artículo 14.
[534] Argentina. Ley 25.326; artículo 42.
[535] Argentina. Ley 25.326; artículo 42 *in fine.*
[536] Argentina. Ley 25.326; artículo 43 (Sentencia).
[537] Argentina. Ley 25.326; inciso 2º del artículo 43

En síntesis, la ley 25.326 aportó un sistema de regulación concreta a la protección de los datos de carácter personal en la República Argentina; aun así, encontramos un derecho que todavía está en formación, y su evolución pasa por la corrección de los defectos y lagunas existentes en la mencionada ley y su decreto reglamentario 1558/2001. Es necesaria la modificación de la ley, luego de una interpretación judicial de la misma, que nos aporte experiencia práctica en casos concretos.

16.- Jurisprudencia

16.1.- Jurisprudencia anterior a la reforma constitucional de 1994

La jurisprudencia en materia de protección de datos personales cuenta con antecedentes anteriores a la reforma constitucional argentina de 1994. El antecedente de mayor relevancia, aun cuando no se refiere expresamente a los datos de carácter personal en sentido restringido, es la sentencia de la Corte Suprema de Justicia de la Nación sobre el caso Ponzetti de Balbín c/ Editorial Atlántida s/ daños y perjuicios.

En este caso están en cuestión los derechos a la imagen y a la intimidad, dado que se debate sobre el derecho de la Editorial Atlántida a publicar una foto del conocido político argentino Ricardo Balbín en la revista Gente Actualidad. La particularidad de la foto ocupa el centro del debate judicial, dado que contiene la imagen de Balbín en momentos en los que agoniza en la terapia intensiva de una clínica de la ciudad de La Plata. Luego de un interesante proceso judicial enriquecido por buenos argumentos a favor de las dos partes enfrentadas en el litigio, la Corte Suprema de Justicia falló a favor al derecho a la intimidad de Balbín, representado por su viuda en esas actuaciones.

Los buenos argumentos planteados entre ambas partes demuestran la dificultad del caso, dado que aparece en forma patente la tensión entre el derecho a

la información y los derechos a la intimidad y a la protección de los datos personales.

Decimos que a pesar de ser un caso resuelto más de diez años antes de la reforma constitucional de 1994, es un fallo sobre datos personales, dado que la imagen de Balbín es un dato personal en los términos del concepto establecido en el artículo 2º de la ley nacional 25326 de Protección de Datos Personales, del año 2000.

16.2.- Jurisprudencia posterior a la reforma constitucional de 1994

Un fallo relevante sobre habeas data posterior a la reforma constitucional de 1994 fue el caso Urteaga, Facundo Raúl contra Estado Nacional - Estado Mayor Conjunto de las FF.AA. - s/amparo ley 16.986, con sentencia de fecha 15 de Octubre de 1998.

En tiempos más recientes, el abogado Ernesto Halabíinterpuso demanda de amparo caratulado "Halabí, Ernesto c/ P.E.N. - ley 25.873 - dto. 1563/04 s/ amparo ley 16.986"[538], en contra de la ley 25.873 y su decreto reglamentario 1563/04. En su opinión, dichos ordenamientos vulneraban las garantías establecidas en los artículos 18 y 19 de la Constitución Nacional, que protegen a las comunicaciones privadas telefónicas y por Internet, en razón de que en ellos no se establecían de manera clara los supuestos en los que éstas podrían ser intervenidas. Además, alegó que esa intromisión constituía una violación a sus derechos de intimidad y privacidad en su condición de usuario y, como abogado, se menoscababa el privilegio de confidencialidad con sus clientes.

En primera instancia se declaró la inconstitucionalidad de los artículos 1° y 2° de la ley y su decreto reglamentario. Según la jueza, no existió un debate legislativo previo al dictado de dicha ley; los antecedentes del derecho comparado

[538] Fallo "Halabi, Ernesto c/ P.E.N. - ley 25.873 - dto. 1563/04 s/ amparo ley 16.986". Op. cit. Fci.:http://www.infojus.gov.ar/index.php?kk_seccion=documento&registro=SUMARIOS&docid=A0071240 (último ingreso el 27/4/2012).

muestran que se han tomado precauciones para no incurrir en violaciones al derecho a la intimidad; las normas de la ley eran vagas, pues no quedaba claro en qué medida las prestadoras de los servicios pueden captar el contenido de las comunicaciones sin la debida autorización judicial y la mala redacción de las mismas dejaba abierta la oportunidad de que los datos captados sean utilizados para fines distintos de los previstos en la ley.

La Sala II de la Cámara Nacional de Apelaciones en lo Contencioso Administrativo confirmó la resolución de primera instancia. Aclaró que la pretensión no se había tornado abstracta, como lo argumentaba el apelante en razón de un decreto que suspendía indeterminadamente al reglamento impugnado, ya que la ley cuestionada seguía vigente, así como el reglamento, remarcando que éste sólo había sido suspendido y no abrogado. La sentencia también precisó que el planteo articulado no era meramente consultivo, sino que existía un interés jurídico del actor como usuario de distintos servicios de telecomunicaciones. En cuanto a la viabilidad de la acción de amparo, consideró que era el medio idóneo para proteger los derechos invocados y respecto al fondo del asunto, hizo suyos los argumentos desarrollados por la Jueza de primera instancia, a los que añadió consideraciones generales sobre el derecho a la intimidad y a la inviolabilidad de la correspondencia. Por último, indicó que la legitimación no excluía la incidencia colectiva de la afectación.

El caso subió a la Corte Suprema de Justicia de la Nación[539], tribunal que el 24 de Febrero de 2009, dictó sentencia considerando que en este asunto existió una adecuada representación de todas las personas, usuarios de los servicios de telecomunicaciones, dentro de los que se encontraban los abogados a los que se extendieron los efectos de la sentencia.Tomó en cuenta la publicidad que se le dio a la audiencia celebrada ante la Corte, como la circunstancia de que la declaración de inconstitucionalidad de la ley 25.873 se encontraba firme y que el decreto reglamentario 1563/04 fue suspendido en su vigencia, que los preceptos

[539] Corte Suprema de Justicia de la Nación (Argentina). Fci.: www.csjn.gov.ar/

constitucionales tanto como la experiencia institucional del país reclamaban el consumo, el goce y ejercicio pleno de las garantías individuales para la efectiva vigencia. Señaló que el artículo 43 de la Constitución Nacional protege tres tipos de derechos diferentes:

1. Derechos divisibles no homogéneos sobre bienes jurídicos individuales

2. Derechos de incidencia colectiva que tienen por objeto proteger bienes colectivos

3. Derechos de incidencia colectiva referentes a intereses individuales homogéneos. En estos casos no hay un bien colectivo, ya que se afectan derechos individuales enteramente divisibles. Sin embargo, hay un hecho, único o continuado, que provoca la lesión a todos ellos y por lo tanto es identificable una causa fáctica homogénea. Ese dato tiene relevancia jurídica porque en tales casos la demostración de los presupuestos de la pretensión es común a todos esos intereses, excepto en lo que concierne al daño que individualmente se sufre. Hay una homogeneidad fáctica y normativa que lleva a considerar razonable la realización de un solo juicio con efectos expansivos de la cosa juzgada que en él se dicte, salvo en lo que hace a la prueba del daño. El juicio correspondiente a la protección de este tipo de derecho sería la acción colectiva o de clase, figura no reconocida en ese momento en el ordenamiento jurídico secundario argentino.

A pesar de no encontrarse regulación secundaria de las acciones colectivas, la Corte Suprema señaló que la disposición constitucional en la que se encuentran previstas es claramente operativa y que es obligación de los jueces darle eficacia, pues donde hay un derecho hay un remedio legal para hacerlo valer, aunque el remedio sea desconocido. Y en tal sentido existen las garantías constitucionales y protegen a los individuos por el sólo hecho de encontrarse en la Constitución. La

falta de reglamentación, dice la Corte, no podrá nunca constituir un obstáculo para la vigencia efectiva de las garantías fundamentales.

Además la Corte argentina establece que en este tipo de juicios el grado de exigencia no podrá ser alto. Así, entonces, la procedencia de este tipo de acciones requiere la verificación de una causa fáctica común, una pretensión procesal enfocada en el aspecto colectivo de los efectos de ese hecho y la constatación de que el ejercicio individual no aparece plenamente justificado. Sin perjuicio de lo cual, también procederá cuando, pese a tratarse de derechos individuales, exista un fuerte interés estatal en su protección, sea por su trascendencia social o en virtud de las particulares características de los sectores afectados. La sentencia expresa que la admisión formal de toda acción colectiva requiere la verificación de ciertos recaudos elementales que hacen a su viabilidad tales como la precisa identificación del grupo o colectivo afectado, la idoneidad de quien pretenda asumir su representación y la existencia de un planteo que involucre, por sobre los aspectos individuales, cuestiones de hecho y de derecho que sean comunes y homogéneas a todo el colectivo. Es esencial, asimismo, que se arbitre en cada caso un procedimiento apto para garantizar la adecuada notificación de todas aquellas personas que pudieran tener un interés en el resultado del litigio, de manera de asegurarles tanto la alternativa de optar por quedar fuera del pleito como la de comparecer en él como parte o contraparte. Es menester, por lo demás, que se implementen adecuadas medidas de publicidad orientadas a evitar la multiplicación o superposición de procesos colectivos con un mismo objeto a fin de aventar el peligro de que se dicten sentencias disímiles o contradictorias sobre idénticos puntos.Posteriormente, el máximo tribunal de justicia argentino analiza el caso en cuestión y concluye que cumple con los requisitos señalados para las acciones colectivas.Realiza el análisis del fondo de la sentencia impugnada, para lo cual usa los criterios de otros países y de instancias internacionales. Concluye que la ley impugnada si violenta las garantías constitucionales y confirma la sentencia del tribunal inferior.

Con los argumentos mencionados la Corte Suprema de Justicia confirmó la sentencia impugnada haciendo lugar al amparo contra la reforma a la ley nacional de telecomunicaciones, por la cual se establecía la obligación de las empresas de telecomunicaciones de resguardar durante diez años la información del tráfico y el contenido de las comunicaciones que realizaban sus abonados sea por teléfono o por Internet (incluyendo el correo electrónico).

En la justicia provincial de la Provincia de Tucumán existe una rica jurisprudencia en materia de protección de datos personales y habeas data. En febrero de 2012, el Juez Civil y Comercial Común de Primera Instancia Raúl Horacio Bejas, dictó un interesante fallo en el juicio "Gasperini, Rubén Orlando c/ Banco Galicia s/ Habeas Data"[540]. El fallo citado hace lugar a la demanda presentada por el actor, dado que la entidad bancaria demanda lo había informado a distintos bancos de información de riesgo de crédito con una calificación negativa y perjudicial para su intimidad. El magistrado justipreció que la demandada contestó el informe requerido, judicialmente, en forma extemporánea y omitiendo presentar prueba de la calificación otorgada al actor. De esta forma, la sentencia consideró al habeas data como una "garantía constitucional específica que tutela el derecho a la intimidad, concepto fundamental de la dignidad humana, cuya protección debe ser eficaz y expeditiva, no dilatoria a partir de excusas procesales ajenas al objetivo constitucional que ha determinado su creación". Para mayor fundamentación menciona al art. 4° de la ley argentina de protección de datos personales N° 25.326, por el cual se establece el principio de calidad de los datos, conforme al cual la información almacenada debe ser adecuada y pertinente, debe estar actualizada "al día", ser exacta, verdadera y en lo posible completa, de acuerdo a la finalidad de su registración. Menciona también esta sentencia que la afectación indebida o por error en un archivo o banco de datos de información de riesgo de crédito, afecta al titular

[540] Fallo "Gasperini, Rubén Orlando c/ Banco Galícia s/ Habeas Data".Expediente N° 1733/11; resuelto por el Juzgado Civil y Comercial Común de Primera Instancia (Justicia Provincial de la Provincia de Tucumán, jurisdicción Capital). Fci.: puede ser consultado en el sitio web del Poder Judicial de la Provincia de Tucumán con el número de expediente: http://www.justucuman.gov.ar/ (último ingreso 2/5/2012).

del dato en sus derechos de acceso inmediato al crédito, en su capacidad crediticia, en el pleno ejercicio del derecho laboral y del derecho asociativo.

Lo relevante de esta sentencia es que el juez expresa que la institución bancaria "está obligada a proceder con absoluta diligencia y a arbitrar todos los medios o actividades necesarias para garantizar la calidad de los datos, (art. 4° de la ley 25.326) y a sustentar con la documentación adecuada e imprescindible que incontrastablemente acredite la legitimidad de su decisión de registrar en mora en un archivo informático de datos personales a un usuario consumidor de sus servicios". En otras palabras, el fallo es prospectivo al recordar, a todas las instituciones bancarias, la obligación de obrar con diligencia, de forma tal que previamente a inscribir un dato descalificador de una persona, tiene que corroborar la documentación cierta que así lo demuestre, conservando tales documentos para el momento en que la justicia o el titular del dato los requiera.

17.- Antecedentes en el derecho público provincial argentino

A partir del diseño constitucional de un sistema de gobierno federal, Argentina cuenta con un doble orden normativo, que distribuye competencias entre el Estado nacional (orden Federal) y los Estados provinciales (orden provincial), de acuerdo con lo establecido por la Constitución Nacional y las constituciones provinciales.

Para delinear un panorama completo de la protección de datos personales en Argentina, resulta de interés conocer las normas constitucionales sobre protección de los datos de carácter personal en las leyes fundamentales de los Estados provinciales.

A partir de 1983, al finalizar el gobierno militar y comenzar un nuevo período democrático, las provincias argentinas realizaron reformas en sus constituciones. Las Constituciones de las provincias de Buenos Aires, Ciudad Autónoma de Buenos Aires, Córdoba, San Juan, Tierra del Fuego y Tucumán,

laincorporaron una garantía de acceso a la información personal contenida en bancos de datos públicos y privados[541], que permite solicitar la rectificación, supresión o actualización de los datos que no fueran correctos.

Un segundo grupo compuesto por las provincias de La Rioja, Salta y San Juan, incorporaron la protección de datos de carácter personal en forma parcial, limitando el instituto a los antecedentes policiales y penales.

Un tercer grupo de constituciones de las provincias de Catamarca, Formosa, San Luis y Río Negro[542], solo abarcaron la protección a las fuentes de información y no protegieron expresamente los datos personales.

Por último, todavía existe un grupo de constituciones provinciales que nada dicen sobre la protección de datos personales, ni del habeas data, aun cuando su articulado se remite a las garantías existentes en la Constitución Nacional.

Antes de reformar su Constitución en el año 2004, la Provincia de Tucumán, a falta de una norma constitucional expresa, protegió los datos de carácter personal pertenecientes a las personas físicas, dentro de su Código Procesal Constitucional[543] a través de un amparo informativo legislado en el artículo 67[544]. Se trata de un amparo especial con plazos procesales especialmente breves.

---

[541] Tejerizo, R. "El Derecho a la intimidad frente la informática". Revista Lex. Ed. Colegio de Abogados de Tucumán, Enero/Febrero de 1998.

[542] Dalla Vía, A.; Basterra, M. I. *Habeas data y otras garantías constitucionales*. Editorial Némesis, Buenos Aires; 1999, p. 65.
Bianchi, A. *Habeas Data y Derecho a la privacidad*. Editorial El Derecho, Buenos Aires; 1995; p. 1.

[543] Vigente a partir de fines de 1999.

[544] Artículo 67 del Código Procesal Constitucional de la Provincia de Tucumán: "cualquier persona física puede reclamar por vía del amparo una orden judicial para conocer las informaciones relativas a su persona que consten en registros o bancos de datos de entidades públicas o privadas destinadas a proveer informes; el destino, uso o finalidad dado a esta información, para actualizar dichas informaciones o rectificar sus errores; para imposibilitar su uso con fines discriminatorios; para asegurar su confidencialidad; para exigir su supresión, o para impedir el registro de datos relativos a sus convicciones ideológicas, religiosas o políticas, a su afiliación partidaria o sindical, su honor, vida privada condición social o racial o intimidad familiar y personal. Será competente para entender en esta acción el Juez en lo Civil y Comercial".

Cabe agregar que las constituciones provinciales reformadas con posterioridad a la reforma de la Constitución Nacional de 1994 han seguido similares principios a los contenidos en la Carta Magna nacional. La Constitución de la Ciudad Autónoma de Buenos Aires[545], en su artículo 16[546], ha legislado un subtipo de amparo más amplio que la acción de habeas data normada por la Constitución Nacional, dado que mientras la Carta Magna nacional habla sólo de "conocer", la ley fundamental de la Ciudad Autónoma de Buenos Aires hace referencia al "libre acceso"[547]. A su vez, el artículo 13 en su inciso 8 de la Constitución de la Ciudad Autónoma de Buenos Aires, establece una tutela especial a la información personal, estableciendo que el secuestro de papeles, correspondencia e información personal almacenada sólo puede ser ordenada por el juez competente.

La Constitución de la Provincia de Buenos Aires[548], reformada en 1994, trata con profundidad el instituto de la protección de datos de carácter personal[549]. Contiene en forma expresa las palabras habeas data en los artículos 20 inc. 3)[550] y

[545] Fci: http://www.senado.gov.ar/web/constituciones/constitucionesprov.html.
[546] Artículo 16 de la Constitución de la Ciudad Autónoma de Buenos Aires: "Toda persona tiene, mediante una acción de amparo, libre acceso a todo registro, archivo o banco de datos que consten en organismos públicos o en los privados destinados a proveer informes a fin de conocer cualquier asiento sobre su persona, su fuente, origen, finalidad o uso que del mismo se haga. También puede requerir su actualización, rectificación, confidencialidad o supresión, cuando esa información lesione o restrinja algún derecho. El ejercicio de este derecho no afecta el secreto de la fuente de información periodística".
[547] Puccinelli, O. (1999). Op. cit., p. 276.
[548] Fci: http://infoleg.mecon.gov.ar/txtnorma/ConstitucionBA.htm
y http://www.senado.gov.ar/web/constituciones/constitucionesprov.html
[549] Dalla Vía, A.; Basterra, M. I. (1999). Op. cit., p.72.
[550] Art. 20 (Constitución de la Provincia de Buenos Aires) "se establecen las siguientes garantías de los derechos constitucionales: 1) ...podrá ejercer la garantía del habeas corpus 2) La garantía del amparo podrá ser ejercida... 3) A través de la garantía del habeas data, que se regirá por el procedimiento que la ley determine, toda persona podrá conocer lo que conste de la misma en forma de registro, archivo o banco de datos de organismos públicos o privados destinados a proveer informes, así como la finalidad a que destine esa información, y a requerir su rectificación, actualización o cancelación. No podrá afectarse el secreto de las fuentes y el contenido de la información periodística. Ningún dato podrá registrarse con fines discriminatorios, ni será proporcionado a terceros, salvo que tengan un interés legítimo. El uso de la informática no podrá vulnerar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos. Todas las garantías precedentes son operativas. En ausencia de reglamentación, los jueces resolverán sobre la procedencia de las acciones que se promuevan, en consideración a la naturaleza de los derechos que se pretendan tutelar.

57. Es esta una de las constituciones del derecho público provincial que tomando como bien jurídico protegido al libre ejercicio de los derechos en general, y en especial a la intimidad personal y familiar. Se diferencia de la Constitución Nacional en los siguientes aspectos: a) Al expresar que se regirá por el procedimiento que la ley determine, estamos ante una norma programática, que se diferencia del modelo normativo de la Constitución Nacional que diseña un habeas data operativo; b) extiende la legitimación activa a los terceros con interés legítimo, mientras que la Carta Magna nacional lo restringe claramente al titular de los datos, al expresar, "de los datos referidos a ella".

Catamarca reformó su Constitución en 1988[551] sin recibir, en este tema, la influencia que causó la Constitución Nacional de 1994. Aun así, la Constitución de Catamarca hace referencia al libre acceso a las fuentes de información en el artículo 11º, el cual textualmente expresa: "La libertad que antecede (en el Art. 10º[552]) comprende el libre acceso a las fuentes de información....". Y aun cuando esta Constitución no hace una referencia expresa, a la protección jurídica de los datos de carácter personal ni al habeas data, a partir de los artículos 39, 40 y 49, cualquier persona puede solicitar la intervención de la justicia al amparo de los derechos y garantías existentes en la Constitución Nacional, entre ellos, la acción de habeas data del art. 43, tercer párrafo.

Córdoba trató en forma general el tema de la protección de los datos de carácter personal en los artículos 47, 48, y 53, al reformar su Constitución en 1987[553]. Esta Constitución incluyó, en forma expresa, la acción de habeas data en su artículo 50[554], con una redacción muy parecida al texto de la Constitución Nacional.

---

[551] Fci.: http://www.infoleg.gov.ar/txtnorma/ConstitucionCatamarca.htm

[552] El artículo 10 de la Constitución de la Provincia de Catamarca establece "Todo habitante de la Provincia es libre de pensar, de escribir. de imprimir o de difundir, por cualquier medio sus ideas, en la medida que no ejercite estos derechos para violar los otros consagrados por esta Constitución, o para atentar contra la reputación de sus semejantes No podrán tampoco fundarse exclusiones e interdicciones de ninguna clase, en diferencias de opiniones o creencias.

[553] Cfr. Fci.: http://infoleg.mecon.gov.ar/txtnorma/ConstitucionCordoba.htm

[554] Art. 50 de la Constitución de la Provincia de Córdoba: "toda persona tiene derecho a conocer lo que de él conste en forma de registro, la finalidad a que se destine esta información y a exigir su

La Constitución de la Provincia de Corrientes[555] no ha incorporado la acción de habeas data, ni hace referencia a la protección jurídica de los datos de carácter personal en su texto. Sin embargo, la protección de los datos de carácter personal puede hacerse efectiva a través de los artículos 184[556] y 185[557], que realizan una remisión expresa a los derechos y garantías establecidos en la Constitución Nacional.

La Constitución de la Provincia de Chaco[558] ha incorporado la acción de habeas data en forma expresa su art. 19[559], con una redacción similar a la existente en el art. 43 tercer párrafo de la Constitución Nacional.

Chubut reformó su Constitución[560] en 1994 y, al igual que las constituciones de su época, incorporó la acción de habeas data en el artículo 56[561], con una redacción idéntica a la existente en la Constitución Nacional. Además de esta

---

actualización y rectificación. Dichos datos no pueden registrarse con propósitos discriminatorios de ninguna clase, ni ser proporcionados a terceros, excepto cuando tengan un interés legítimo. La ley reglamenta el uso de la informática para que no se vulnere el honor ni la intimidad personal, familiar y el pleno ejercicio de los derechos".

[555] Confrontar con el sitio web:http://infoleg.mecon.gov.ar/txtnorma/Constitucionde Corrientes.htm

[556] Artículo 184 de la Constitución de la Provincia de Corrientes: "Hasta tanto se dicte la legislación pertinente, se aplicará el régimen de la ley de amparo para la efectiva protección inmediata y expeditiva de los derechos y garantías contenidos en las cláusulas operativas de los tratados y convenciones internacionales, que hayan sido objeto de ratificación o adhesión por parte de la República Argentina, sin que puedan incluirse o comprenderse otros reclamos con tal motivo".

[557] Artículo 185 de la Constitución de la Provincia de Corrientes: "Mientras no se dicte la ley reglamentaria de una libertad o garantía declarada por esa Constitución y la omisión sea irrazonable quien se considera afectado por ella en su derecho individual o colectivo podrá solicitar o deberá obtener que la garantía o libertad integre el orden normativo, con efecto limitado a la contienda judicial y al solo fin de decidirla".

[558] Cfr. Fci.: http://infoleg.mecon.gov.ar/txtnorma/ConstitucionChaco.htm

[559] Art. 19 de la Constitución de la Provincia de Chaco: "toda persona tiene derecho a informarse de los datos que sobre sí mismo o sobre sus bienes obren en forma de registro o sistemas oficiales o privados de carácter público, la finalidad a que se destine esa información, y a exigir su actualización, corrección, supresión o confidencialidad. Tales datos no podrán ser utilizados con fines discriminatorios de ninguna especie. No podrá afectarse el secreto de las fuentes de información periodística".

[560] Cfr.Fci.: http://www.sup-trib-delsur.gov.ar/sup-trib-delsur/cbconst.htm

[561] Artículo 56 de la Constitución de la Provincia de Chubut: "Toda persona puede interponer acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o en los privados destinados a proveer información, y en caso de error, omisión, falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No puede afectarse el secreto de la fuente de información periodística".

norma expresa, los artículos 54, 55, y 61 también hacen una referencia indirecta a la protección de datos personales.

La Constitución de la Provincia de Entre Ríos sancionada en 1993[562] no hace una mención expresa del habeas data, pero al igual que otras constituciones que aún no han legislado expresamente esta garantía, permite la protección de los datos de carácter personal por medio de los artículos que reconocen los derechos y garantías establecidos por la Constitución Nacional.

La Provincia de Formosa reformó su Constitución en 1991[563], y no incorporó la acción de habeas data ni legisló en forma expresa sobre la protección de datos de carácter personal. Sin embargo, incluyó, en el artículo 10[564], un derecho de habeas data impropio para permitir a todos los habitantes de la Provincia el libre acceso a las fuentes de información. Los artículos 5, 17 y 23 contienen principios aptos para una protección indirecta de los datos de carácter personal.

La Constitución de la Provincia de Jujuy[565]legisló en forma expresa sobre la protección de los datos de carácter personal en su artículo 23, referido a la protección de la intimidad, de la honra y dignidad. Este artículo destina dos incisos a la protección de los datos personales: el inc. 6º[566], a través del cual se incluye una acción de habeas data, instrumentada como garantía constitucional; y el inc. 8[567], por el cual se prohíbe el procesamiento de datos sensibles.

---

[562] Fci.: http://infoleg.mecon.gov.ar/txtnorma/ConstitucionEntreRios.htm

[563] Constitución de la Provincia de Formosa.
Fci.: http://infoleg.mecon.gov.ar/txtnorma/ConstitucionFormosa.htm.

[564] Artículo 10 de la Constitución de la Provincia de Formosa: "Todos los habitantes de la Provincia gozan del derecho al libre acceso a las fuentes de información"

[565] Cfr.Fci.: http://infoleg.mecon.gov.ar/txtnorma/ConstituciondeJujuy.htm

[566] Artículo 23, inciso 6º de la Constitución de la Provincia de Jujuy: "Todas las personas tienen derecho a tomar conocimiento de lo que constare a su respecto en los registros provinciales de antecedentes personales y del destino de estas informaciones, pudiendo exigir la rectificación de los datos. Queda prohibido el acceso de terceros a estos registros, así como su comunicación, salvo en los casos expresamente previstos por la ley".

[567] Artículo 23, inciso 8 de la Constitución de la Provincia de Jujuy: "El procesamiento de datos por cualquier medio o forma nunca puede ser utilizado para su registro y tratamiento con referencia a convicciones filosóficas, ideológicas o políticas, filiación partidaria o sindical, creencias o respecto

La legislatura jujeña reglamentó la Constitución Provincial por medio de la ley 4.444, en su artículo 10º instrumentó el derecho al acceso a las fuentes de información, también llamado habeas data impropio. En agosto de 2000, el parlamento jujeño también sancionó la ley Nº 5188 de regulación de la acción de amparo de habeas data, a partir de la cual toda persona física o jurídica que acredite tener un interés legítimo puede solicitar sus datos personales o íntimos ante cualquier registro o banco de datos públicos o privados y pedir su eliminación, corrección o ampliación. El art. 2º de esta ley, también otorga legitimación activa a los herederos hasta el cuarto grado de consanguinidad y al cónyuge, siempre que no estuviere divorciado de la persona cuyos derechos resulten afectados[568].

La Provincia de La Pampa[569]reformó en 1994 su Constitución sancionada en 1960. La reforma de 1994 no incluye en forma expresa ni la protección de los datos personales, ni crea una garantía especial de habeas data. Sin embargo, el texto constitucional permite aplicar el habeas data existente en la Constitución Nacional, por medio de los artículos 16[570] y 17 entre otros. El art. 17 ordena que los jueces presten amparo a todo derecho reconocido por las constituciones de la Nación o de la Provincia y si no hubiere reglamentación o procedimiento legal deben arbitrar los trámites breves a tal efecto.

La Constitución de la Provincia de La Rioja[571] sancionada el 14 de Agosto de 1926 y reformada por medio de la Convención de 1998, permite observar la influencia recibida del derecho español, y en especial el art. 18 de la constitución española sobre el derecho a la intimidad. Prácticamente repite la primera parte del

---

de la vida privada, salvo que se tratare de casos no individualmente identificables y para fines estadísticos".

[568] Antecedentes Parlamentarios, *Ley 25326. Habeas Data*. Editorial La Ley año VII – N° 11 – Diciembre de 2000; p. 512.

[569] Fci.: http://www.lapampa.gov.ar/CConstit.htm.

[570] Art 16 de la Constitución de la Provincia de La Pampa expresa: "Todo habitante por sí o por intermedio de otra persona, que no necesitará acreditar mandato ni llenar formalidad procesal alguna, y a cualquier hora, podrá reclamar al juez más inmediato sin distinción de fueros ni de instancias, que se investiguen la causa y el procedimiento de cualquier restricción o amenaza real a su libertad personal. Inmediatamente el juez hará comparecer al recurrente y comprobada en forma sumarísima la violación, hará cesar sin más trámite la restricción o amenaza. En los mismos casos los jueces podrán expedir de oficio mandamiento de habeas corpus".

[571] Fci.: http://www.senado.gov.ar/web/constituciones/larioja/larioja.html

texto redactado por el constituyente español, el cual ordena que la ley limite el uso de la informática para preservar el honor, la intimidad personal y familiar de los habitantes y el pleno ejercicio de sus derechos. Las autoridades sólo proporcionarán antecedentes penales de los habitantes en los casos previstos por la ley.

La Constitución de la Provincia de Mendoza[572], sancionada en el año 1916 y reformada en 1965, aún no ha incorporado en forma expresa la protección jurídica de los datos de carácter personal. Sin embargo, la legislación provincial hace referencia al habeas data en el art. 474 del Código Procesal Penal de la Provincia[573], donde manifiesta que se regirá por las disposiciones que se establecen para el habeas corpus.

La Constitución de Misiones[574], sancionada en 1958, no legisló expresamente sobre la protección de los datos de carácter personal, ni estableció una garantía constitucional de habeas data. Sin embargo, cabe una protección indirecta a través del artículo 7[575] que otorga a todos los habitantes de la Provincia los derechos y garantías reconocidos por la Constitución Nacional. Y en igual sentido, son de aplicación indirecta los artículos 16[576], 17[577] y 18[578] relativos a los recursos de

[572] Fci.: http://www.mendoza.gov.ar/.

[573] Ley de la Provincia de Mendoza N° 1908 "Código Procesal Penal de la Provincia de Mendoza", Libro Tercero Título II, Juicios especiales. Capitulo V. Habeas Corpus. Artículo 474: "Toda persona detenida o incomunicada, en violación de los artículos 28, 29, 30, y correlativos de la Constitución Provincial, o que considere inminente su detención arbitraria, podrá interponer habeas Corpus para obtener que cese la restricción o la amenaza. Igual derecho tendrá cualquiera otra persona, para demandar por el afectado sin necesidad de poder.
Cuando el habeas corpus tuviere como fundamento el re-agravamiento de las condiciones de prisión impuestas por órgano judicial competente, se procederá de conformidad con la ley nacional N° 23.098. En lo pertinente, el habeas data se regirá por las disposiciones contenidas en el presente capitulo. Fuente: SAIJ (Sistema Argentino de Informática Jurídica) www.saij.jus.gov.ar

[574] Fci.: http://www.misiones.gov.ar/poder_legislativo/constitucion.htm

[575] Artículo 7º de la Constitución de la Provincia de Misiones: "Los habitantes de la Provincia gozan de todos los derechos y garantías reconocidos en la Constitución Nacional, con arreglo a las leyes que reglamenten su ejercicio".

[576] Artículo 16 de la Constitución de la Provincia de Misiones: "Frente a cualquier decisión o acto arbitrario de la autoridad, en relación tanto a la persona como a los derechos de los habitantes de la Provincia, y ya se trate de una lesión jurídica consumada como de una amenaza inminente, proceden los recursos de habeas-corpus o de amparo a los fines de que cese el efecto de lo ya consumado o no se lleve a cabo lo amenazado".

[577] Artículo 17 de la Constitución de la Provincia de Misiones: "Los recursos a que se refiere el artículo anterior podrán ser interpuestos por el interesado o cualquier persona, sin necesidad de

amparo que pueden ser interpuestos por el interesado y por cualquier otra persona, con un trámite breve y sumarísimo, y sin necesidad de observar formas procesales.

La Provincia de Neuquén, reformó en marzo de 1994 su Constitución sancionada en 1957[579] y no incluyó la protección de los datos personales ni la acción de habeas data en su texto reformado. Sin embargo, se puede alcanzar una protección jurídica indirecta de los datos de carácter personal, aplicando el artículo 32, referido al secreto y a la seguridad de las comunicaciones[580], y el artículo 51[581], que impide la alteración, limitación y restricción de los derechos y garantías consagrados por la Constitución Nacional.

La Constitución de la Provincia de Río Negro[582] protege el derecho a la intimidad y asegura el acceso de las personas afectadas a la información para su rectificación, actualización o cancelación cuando no fuera razonable su mantenimiento en el artículo 20[583]. Este mismo artículo ordena que una ley reglamente el uso de la información bajo los principios de justificación social, limitación de la recolección de datos, calidad, especificación del propósito,

---

observar formas procesales, ante cualquier juez letrado de primera instancia, sin distinción de fueros o circunscripciones".

[578] Artículo 18 de la Constitución de la Provincia de Misiones: "Tanto en el caso de habeas-corpus como en el de amparo de cualquier derecho, el trámite de recurso será breve y sumarísimo, siendo responsable el juez que en él entienda de toda dilación inconducente o injustificada".

[579] Fci.: http://www.neuquen.gov.ar/pagina_de_constitucion_provincial/constitucion_provincial.htm

[580] Artículo 32 de la Constitución de Neuquén: "Se declara inviolable la seguridad individual. Con ese carácter serán respetados: la conciencia, la integridad física, la defensa en juicio, la correspondencia de toda índole, los papeles privados, las comunicaciones telefónicas, telegráficas, cablegráficas u originadas por cualquier otro medio, así como el normal ejercicio del trabajo, profesión o medios de vida.

[581] Artículo 51 de la Constitución de la Provincia de Neuquén: **"**Los derechos y garantías consagrados por esta Constitución y por la Constitución Nacional, no podrán ser alterados, restringidos ni limitados por las leyes que reglamenten su ejercicio".

[582] Cfr. Fci.: http://www.legisrn.gov.ar/.

[583] Artículo 20 de la Constitución de la Provincia de Río Negro: "La ley asegura la intimidad de las personas. El uso de la información de toda índole o categoría, almacenada, procesada o distribuida por cualquier medio físico o electrónico debe respetar el honor, la privacidad y el goce completo de los derechos. La ley reglamenta su utilización de acuerdo a los principios de justificación social, limitación de la recolección de datos, calidad, especificación del propósito, confidencialidad, salvaguardia de la seguridad, apertura de los registros, limitación en el tiempo y control público. Asegura el acceso de las personas afectadas a la información para su rectificación, actualización o cancelación cuando no fuera razonable su mantenimiento".

confidencialidad, salvaguardia de la seguridad, apertura de registros, limitación en el tiempo y control público. Este mandamiento constitucional fue cumplido por medio de la ley provincial Nº 3.246.

La Constitución de la Provincia de Salta[584] incorporó la protección de los datos de carácter personal recién a partir de la reforma realizada en 1998, que incluye al habeas data como garantía constitucional en el artículo 89[585]. En esta norma se faculta a "toda persona" para interponer la acción de habeas data, en forma expedita, con el objeto de tomar conocimiento de los datos referidos a ella o a sus bienes, y de la finalidad para la cual están registrados. Para que proceda la acción de habeas data, los datos objeto de ella deben estar almacenados en registros o bancos de datos públicos o privados, destinados a proveer informes. Esta Constitución estipula que en caso de detectarse la presencia de datos falsos, erróneos, obsoletos o de carácter discriminatorio, el sujeto activo podrá exigir la supresión, rectificación, confidencialidad o actualización de aquellos.

La Constitución de la Provincia de San Juan[586] estatuye en su art. 19 que toda humillación a la persona por motivos de instrucción, condición socio-económica, edad, sexo, raza, nacionalidad, religión, ideas o por cualquier otra causa, será castigada severamente. La incorporación de la garantía del *habeas data* se ubica en el apartado referido al Registro de Personas e Informática, regulado en el artículo 26 de la Constitución[587]. A su vez, el art. 27[588] de la Constitución sanjuanina otorga a

[584] Fci.: http://www.gobiernosalta.gov.ar/salta.html.
[585] Artículo 89. - *Habeas Data*. Toda persona podrá interponer acción expedita de habeas data para tomar conocimiento de los datos referidos a ella o a sus bienes, y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes. En caso de datos falsos, erróneos, obsoletos o de carácter discriminatorio, podrá exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".
[586] Fci.: http://infoleg.mecon.gov.ar/txtnorma/ConstitucionSanJuan.htm
[587] Artículo 26 de la Constitución de la Provincia de San Juan: **"**Todo ciudadano tiene derecho a tomar conocimiento de lo que de él conste en forma de registro y de la finalidad a que se destinan las informaciones, pudiendo exigir la rectificación de datos, así como su actualización. No se puede utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se destine para fines estadísticos no identificables".
[588] Artículo 27 de la Constitución de la Provincia de San Juan: "Todos los habitantes tienen derecho a que se les informe veraz y auténticamente sin distorsiones de ningún tipo, teniendo también el

todas las personas el derecho de acceso a la información pública, instituto conocido como habeas data impropio.

San Luis sancionó su Constitución el 26 de marzo de 1987[589], incorporando la acción de *habeas data* en el artículo 21[590]. Esta norma establece que todos los habitantes tienen derecho a tomar conocimiento de lo que de ellos conste en registros de antecedentes personales e informarse sobre la finalidad a que se destinan dichos registros y la fuente de información en la que se obtienen los datos respectivos.

Este artículo ha sido criticado por ser limitado e incompleto. Limitado, por restringir la legitimación activa a los habitantes. Incompleto, porque luego de otorgar el derecho a conocer los datos, la fuente de información y la finalidad de los registros, no establece lo que puede hacer el afectado si se produce una violación a sus derechos por la actividad mencionada. A pesar de las críticas indicadas, no debemos perder de vista que esta Constitución fue sancionada en 1987[591], tiempos en los cuales existían muy pocos antecedentes sobre la protección de los datos de

---

derecho al libre acceso a las fuentes de información, salvo en asuntos vitales para la seguridad del Estado. El tiempo de la reserva se fijará por ley. La información en todos sus aspectos es considerada como de interés público".

[589] Fci.: http://infoleg.mecon.gov.ar/txtnorma/ConstitucionSL.htm

[590] Artículo 21: Libertad de expresión y derecho de información
Es inviolable el derecho que toda persona tiene de expresar libremente sus ideas y opiniones y de difundirlas por cualquier medio, sin censura de ninguna clase. Ninguna ley ni autoridad puede restringir la libre expresión y difusión de las ideas, ni trabar, impedir ni suspender por motivo alguno el funcionamiento de los talleres de impresión, difusoras radiales, televisivas y demás medios idóneos para la emisión y propagación del pensamiento, ni secuestrar maquinarias o enseres, ni clausurar sus locales, salvo por resolución judicial. Aquel que abuse de este derecho es responsable de los delitos comunes en que incurre a su amparo y de la lesión que cause a quiénes resulten afectados. Todos los habitantes de la Provincia gozan del derecho al libre acceso a las fuentes públicas de información. La libertad de expresión comprende también el derecho de las publicaciones a obtener los elementos necesarios a tal fin, y la facultad que tiene toda persona a la réplica o rectificación ante una referencia o información susceptible de afectar su reputación personal, la que debe publicarse gratuitamente, en igual forma y con el mismo medio utilizado. Una ley especial asegura la protección debida a toda persona o entidad contra los ataques a su honra, reputación, vida privada o familiar, cuando ésta es lesionada por cualquiera de los medios de difusión determinados en este artículo. Todos los habitantes de la Provincia tienen derecho a tomar conocimiento de lo que de ellos conste en registro de antecedentes personales e informarse sobre la finalidad a que se destinan dichos registros y la fuente de información en que se obtienen los datos respectivos.

[591] Constitución de la Provincia de San Luis. Sancionada el 26 de Marzo de 1987 y publicada en el Boletín Oficial de la Provincia de San Luis del día 8 de Abril de 1987.

carácter personal en Argentina y muy poca legislación comparada en América. Aceptadas estas observaciones, la constitución bajo análisis puede ser considerada como un antecedente y un aporte importante para los tiempos en los cuales fue dictada.

Otros artículos en la Constitución de la Provincia de San Luis, (10, 42, 45, y 46) tienen una relación indirecta con la protección jurídica de los datos de carácter personal.

La Constitución de la Provincia de Santa Cruz[592] fue reformada en el año 1994 y aun cuando entre sus enmiendas no incorpora la acción de *habeas data*, sí contiene normas como el artículo 6º[593], que ordenan cumplir con los derechos y garantías de la Constitución Nacional. En igual sentido, el artículo 15[594] establece que los jueces prestarán amparo a todo derecho reconocido en la Constitución Nacional. Siguiendo esta línea, el artículo 18 autoriza a los jueces a dictar un mandato de ejecución contra la autoridad que se niegue a dar cumplimiento a una obligación legal que afecte a un particular[595].

Los damnificados por el incumplimiento de un derecho o garantía constitucional, tienen a partir del artículo 17º[596] de la Constitución de Santa Cruz,

---

[592] Honorable Cámara de Diputados de la Provincia de Santa Cruz.
Fci.: http://www.hcdsc.gov.ar/html/constitucion_provincial.asp.

[593] Artículo 6º de la Constitución de Santa Cruz: "En ningún caso podrán las autoridades de la Provincia suspender la observancia de esta Constitución ni de la Nacional, ni la efectividad de las garantías y derechos establecidos en ambas. En caso de Intervención Federal, los actos practicados por el Interventor serán válidos si hubieren sido realizados conforme a esta Constitución y Leyes de la Provincia."

[594] Artículo 15 de la Constitución de la Provincia de Santa Cruz: "los jueces prestarán amparo a todo derecho reconocido en la Constitución Nacional y ésta, si no hubiera reglamentación o procedimiento legal, arbitrará a ese efecto trámites breves".

[595] El artículo 18º de la Constitución de Santa Cruz, establece que "siempre que una ley u ordenanza imponga a un funcionario o corporación pública de carácter administrativo un deber expresamente determinado, todo aquel que en cuyo interés deba ejecutarse el acto o sufriere perjuicio material, moral o político, por falta de cumplimiento del deber, puede demandar ante los Tribunales su ejecución inmediata y el Tribunal, previa comprobación sumaria de la obligación legal y del derecho del reclamante, dirigirá al funcionario o corporación un mandamiento de ejecución".

[596] Artículo 17 de la Constitución de Santa Cruz: "toda ley, decreto u orden contrarios a los principios, derechos o garantías que esta Constitución consagra, no podrán ser aplicados por los Jueces. Todo individuo que por tales leyes, decretos u órdenes sea lesionado en sus derechos, tiene

una acción civil para pedir indemnización por los perjuicios que se les hayan causado contra el empleado, funcionario o mandatario que los hubiera dictado, autorizado o ejecutado.

La Provincia de Santiago del Estero sancionó la reforma de su Constitución[597] en 1997, entrando en vigencia el 30 de diciembre de ese año. La Carta Magna santiagueña, dedica el artículo 16 a los derechos individuales y en su artículo 3º hace expresa referencia al derecho al honor, a la intimidad, al nombre y a la propia imagen.

Pero es en el artículo 60[598], donde reconoce el derecho de toda persona a interponer acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad, siempre que ellos consten en registros o bancos de datos públicos o en los privados destinados a proveer informes. En caso de existir error, omisión, falsedad o discriminación en los datos almacenados permite exigir la supresión, rectificación, confidencialidad o actualización de aquellos.

La Constitución de la Provincia de Tierra del Fuego, Antártida e Islas del Atlántico Sur[599], sancionada el 17 de mayo de 1991, protege los datos de carácter personal, por medio de una garantía constitucional de habeas data, y de otras normas relativas al tema. La acción de habeas data se encuentra ubicada en el artículo 45[600], el cual manifiesta en forma expresa que toda persona tiene derecho a

---

acción civil para pedir indemnización por los perjuicios que se le hayan causado, contra el empleado, funcionario o mandatario que los hubiera dictado, autorizado o ejecutado".

[597] Constitución de la Provincia de Santiago del Estero.
Fci.: http://www.senado.gov.ar/web/constituciones/santiagodelestero/santiagodel.html

[598] Artículo 60 de la Constitución de Santiago del estero: *HABEAS DATA*. Toda persona puede interponer acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o en los privados destinados a proveer informes y en caso de error, omisión, falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No puede afectarse el secreto de la fuente de información periodística.

[599] Poder Legislativo de la Provincia de Tierra del Fuego, Antártida e Islas del Atlántico Sur. Fci.: http://www.legistdf.gov.ar/

[600] Art. 45 de la Constitución de Tierra del Fuego, Islas Malvinas e islas del Atlántico Sur: "Toda persona tiene derecho a conocer lo que de ella conste en forma de registro y la finalidad a que se destine esa información, y a exigir su rectificación y actualización. Estos datos no pueden

conocer lo que de ella conste en forma de registro y la finalidad a que se destine esa información, y a exigir su rectificación y actualización.

La Constitución de la Provincia de Santa Fe[601], sancionada el 14 de abril de 1962, en tiempos en los cuales no existían antecedentes nacionales en materia de protección de datos de carácter personal, no contiene una norma expresa que los proteja. Sin embargo, los datos de carácter personal están protegidos por los artículos de la Constitución Provincial que reconocen los derechos o garantías existentes en la Constitución Nacional. Una de estas normas es el artículo 17[602] de la Constitución Provincial, que autoriza a plantear un recurso jurisdiccional de amparo contra cualquier decisión, acto u omisión de una autoridad administrativa provincial, municipal o comunal, o de entidades o personas privadas en ejercicio de funciones públicas, que amenazare, restringiere o impidiere, de manera manifiestamente ilegítima, el ejercicio de un derecho de libertad directamente reconocido a las personas en la Constitución de la Nación o de la Provincia, siempre que no pudieren utilizarse los remedios ordinarios sin daño grave e irreparable y no existieren recursos específicos de análoga naturaleza acordados por leyes o reglamentos.

17.1.- Protección de datos en la Provincia de Tucumán (Argentina)

Al formar parte de la República Argentina, la Provincia de Tucumán participa de un sistema de gobierno representativo, republicano y federal, conforme

---

registrarse con propósitos discriminatorios de ninguna clase ni ser proporcionados a terceros, excepto cuando estos tengan un interés legítimo".

[601] Dalla Vía, A.; Basterra, M. (1999). Op. cit., p. 85. En esta obra se puede consultar el texto completo de la ley 24.745.
Ver. Fci.:http://www.senado.gov.ar/web/constituciones/santafe/santafe.html

[602] Artículo 17 de la constitución de la Provincia de Santa Fe: "Un recurso jurisdiccional de amparo, de trámite sumario, puede deducirse contra cualquier decisión, acto u omisión de una autoridad administrativa provincial, municipal o comunal, o de entidades o personas privadas en ejercicio de funciones públicas, que amenazare, restringiere o impidiere, de manera manifiestamente ilegítima, el ejercicio de un derecho de libertad directamente reconocido a las personas en la Constitución de la Nación o de la Provincia, siempre que no pudieren utilizarse los remedios ordinarios sin daño grave e irreparable y no existieren recursos específicos de análoga naturaleza acordados por leyes o reglamentos".

lo establece el artículo 1° de la Constitución Nacional. La forma de gobierno federal está basada en la división del poder entre el gobierno federal y los gobiernos locales, conservando las provincias "todo el poder no delegado por esta Constitución al Gobierno Federal" (Constitución Nacional, Art. 121). El sistema federal permite el control y la cooperación recíproca entre las provincias y el gobierno federal, evitando la concentración de poder a través de su descentralización. En este sistema, coexisten dos clases de gobierno: el nacional o federal, soberano, cuya jurisdicción abarca todo el territorio de la Nación, y los gobiernos locales, autónomos en el establecimiento de sus instituciones y sus constituciones locales, cuyas jurisdicciones abarcan exclusivamente sus respectivos territorios.

Por la adopción del sistema de gobierno federal, se produce en argentina una distribución de competencias legislativas, a partir de la cual le compete al gobierno nacional o federal la aprobación de las leyes de fondo o también llamado derecho de sustancia y a los gobiernos locales o provinciales, además del dictado de sus constituciones, la legislación de forma o también llamado derecho adjetivo.

La anterior Constitución de Tucumán de 1990 no aludía en forma directa al habeas data, pero su artículo 22º, primera parte, expresaba que todos los habitantes de la Nación Argentina, al amparo de la Constitución Nacional, podían ejercer los derechos que ella establece. Y puesto que a partir de 1994, la Constitución Nacional había incorporado el habeas data en su artículo 43 tercer párrafo, podemos decir que a partir de ese momento, la Constitución de Tucumán hacía referencia en forma indirecta al habeas data de la Constitución Nacional.

Además, el artículo 34 de la Constitución tucumana de 1990, autorizaba a solicitar el amparo a los jueces en la forma que determine la ley, siempre que en forma actual o inminente se restrinjan, amenacen o lesionen con arbitrariedad o ilegalidad manifiesta, los derechos o las garantías reconocidos por la Constitución Provincial o Nacional y no exista otra vía pronta o eficaz para evitar un grave daño. La Provincia de Tucumán promulgó en diciembre del año 2004 la ley 7469 por la

cual se declaró la necesidad de reformar la Constitución provincial a los efectos de modificar, suprimir o incorporar disposiciones, entre las cuales el punto IV de la ley autorizaba en su apartado 7º la incorporación del habeas data a los efectos de lograr una tutela legal y judicial eficaz. La llegada tardía del habeas data invitaba a un análisis serio del tema, para no repetir las falencias de otras constituciones y colocar a la Provincia de Tucumán en un lugar de avanzada tanto en el contexto de las legislaciones o Constituciones provinciales y en el derecho comparado americano. Finalmente la Provincia de Tucumán reformó su Constitución en el año 2006, incorporando el instituto del habeas data en su artículo 39 con el siguiente texto: "Toda persona podrá interponer acción expedita de Habeas Data para tomar conocimiento de los datos referidos a ella o a sus bienes y su finalidad, que consten en registros o bancos de datos públicos o privados. En caso de datos falsos, erróneos, obsoletos, incompletos o de carácter discriminatorio podrá exigir su supresión, rectificación, confidencialidad, adición o actualización. En ningún caso podrá afectarse el secreto de las fuentes de información periodística. Ningún dato podrá registrarse con fines discriminatorios, ni será proporcionado a terceros salvo que tengan un interés legítimo. El uso de los registros informáticos y de otras tecnologías no podrá vulnerar el honor, la intimidad personal y familiar, y el pleno ejercicio de los derechos".

Antes de reformar la Constitución en el año 2006, la Provincia de Tucumán ya contaba con el recurso de Amparo Informativo incorporado en el año 1995 dentro del Código Procesal Constitucional de la Provincia. En el mencionado digesto procesal constitucional se regulaba como la acción de habeas data como una especie de amparo. El mencionado Código fue promulgado el 2 de marzo y publicado en el 8 de marzo de 1999. La inusual demora en promulgar y publicar una ley con casi cuatro años de demora, alerta sobre las razones políticas que retrasaron la puesta en práctica de esta norma. La reforma de la Constitución de 1994 no figura entre los antecedentes mencionados en la exposición de motivos, dado que la elaboración del proyecto fue previa a esa reforma constitucional nacional. Sin embargo, no existen incompatibilidades entre la enmienda nacional y el Código

Procesal Constitucional tucumano y, más aún, en materia de protección de datos personales se anticipó a lo dispuesto tiempo después en la convención de Santa Fe-Paraná, reformadora de la Constitución Nacional en 1994.

El Código Procesal Constitucional de la Provincia de Tucumán sistematizó los diversos mecanismos de tutela de los derechos humanos, y contempla en el capítulo IV, dentro de los amparos especiales, el artículo 67 sobre amparo informativo o habeas data. Actualmente, ante la falta de adhesión provincial a la ley 25.326, el amparo informativo es la vía idónea para la protección de los datos de carácter personal en los tribunales de la Provincia de Tucumán

Posteriormente, en Junio de 2006, la Provincia de Tucumán aprobó la Reforma a la Constitución de 1990. Sobre la Constitución de 2006 de Tucumán y la protección de datos personales nos ocuparemos más adelantes, dado que antes encontramos un importante antecedente para la materia de estos estudios en el año 1995, año en el cual la legislatura de la Provincia de Tucumán sancionó el Código Procesal Constitucional, que regula la acción de habeas data como una especie de amparo.

El Código mencionado fue promulgado el 2 de marzo de 1995 y curiosamente publicado recién cuatro años más tarde, el 8 de marzo de 1999. La inusual demora en promulgar y publicar una ley con casi cuatro años de retraso, alerta sobre las razones políticas que generaron resistencia a la puesta en práctica de esta norma[603].

La reforma de la Constitución de 1994 no figura entre los antecedentes mencionados en la exposición de motivos dado que la elaboración del proyecto[604] fue realizada incluso antes de la reforma constitucional nacional. Sin embargo no

[603] Sagués, N. "El nuevo Código Procesal Constitucional de la Provincia de Tucumán". Publicado en la Revista de Derecho Procesal: "Amparo, habeas data, habeas corpus – I" Editorial Rubinzal-Culzoni Editores; Santa Fe (Argentina), marzo de 2000; pp. 443-462.

[604] El autor del Proyecto del Código Procesal Constitucional de la Provincia de Tucumán, fue el Profesor Titular de la Cátedra A de Derecho Constitucional de la Universidad Nacional de Tucumán, Dr. Sergio Díaz Ricci.

existen incompatibilidades entre la enmienda nacional y el Código Procesal Constitucional tucumano y, más aún, en materia de protección de datos personales se anticipó a lo dispuesto tiempo después en la convención de Santa Fe-Paraná reformadora de la Constitución Nacional en 1994.

El Código Procesal Constitucional de Tucumán es un importante avance en la sistematización de los diversos mecanismos de tutela de los derechos humanos[605] y contempla, en el capítulo IV, dentro de los amparos especiales, el artículo 67[606] sobre amparo informativo o habeas data; habitualmente usado como una herramienta para asegurar el respeto a los derechos a la intimidad y a la protección de los datos de carácter personal. Cabe destacar que, ante la falta de adhesión provincial a la ley 25.326, el amparo informativo es la vía idónea y el rito o procedimiento para la protección de los datos de carácter personal en los tribunales provinciales de Tucumán.

Textualmente el artículo 67 del Código Procesal Constitucional de la Provincia expresa: "(Amparo Informativo - habeas data). Cualquier persona física puede reclamar por vía del amparo, una orden judicial para conocer las informaciones relativas a su persona, que consten en registros o bancos de datos de entidades públicas o privadas, destinada a proveer informes; el destino, uso o finalidad dado a esa información, para actualizar dichas informaciones o rectificar sus errores; para imposibilitar su uso con fines discriminatorios, para asegurar su confidencialidad, para exigir su supresión o para impedir el registro de datos relativos a sus convicciones ideológicas, religiosas o políticas, a su afiliación partidaria o sindical, o a su honor, vida privada, condición social o racial o

[605] El Código Procesal Constitucional de la Provincia de Tucumán, es un conjunto de herramientas para asegurar el respeto a la Constitución, por el Estado y los particulares. En una única ley se reúnen procedimientos antes dispersos en leyes y códigos (habeas corpus, amparos en general, amparo electoral, recurso de inconstitucionalidad) con nuevos instrumentos entre los que se encuentra el amparo informativo o (habeas data) La totalidad de los procesos y recursos constitucionales se han unificados y ordenado sistemáticamente en este Código Procesal Constitucional, cuyo objeto es simplificar y dar celeridad a los trámites.

[606] Artículo 67 del Código Procesal Constitucional de la Provincia de Tucumán: Amparo Informativo - habeas data.

intimidad familiar y personal. Será competente para conocer en esta acción, el juez en lo civil o comercial común".

En diciembre del año 2004, la Legislatura Provincial sancionó la ley 7469, por la cual se declaraba la necesidad de reformar la Constitución provincial, con el propósito de modificar, suprimir o incorporar disposiciones, entre las cuales el punto IV de la ley autorizaba en su apartado 7º la incorporación del *habeas data*, a los efectos de lograr una tutela legal y judicial eficaz. Esta convocatoria fue un desafío abierto a los constituyentes tucumanos para incorporar este nuevo derecho en su Constitución. Pesaron los antecedentes internacionales, nacionales y provinciales, para la incorporación del habeas data a la nueva Constitución tucumana, finalmente aprobada el 6 de Junio del año 2006[607].

La nueva carta magna tucumana incluye en su artículo 39 el instituto del *habeas data*con el siguiente texto: "Toda persona podrá interponer acción expedita de Habeas Data para tomar conocimiento de los datos referidos a ella o a sus bienes y su finalidad, que consten en registros o bancos de datos públicos o privados.En caso de datos falsos, erróneos, obsoletos, incompletos o de carácter discriminatorio podrá exigir su supresión, rectificación, confidencialidad, adición o actualización. En ningún caso podrá afectarse el secreto de las fuentes de información periodística".

Como podemos observar, el nuevo texto del artículo 39 de la Constitución de la Provincia de Tucumán del año 2006, sigue la matriz del artículo 43 tercer párrafo de la Constitución de la Nación Argentina (1994). Sin embargo, podemos resaltar algunas diferencias:

a) Mientras la Constitución Argentina evita mencionar el nombre del instituto (*habeas data*) en el texto del artículo 43. La Constitución de la Provincia de Tucumán lo menciona en forma expresa.

[607] Argentina, Constitución de la Provincia de Tucumán (2006).
Fci.: http://rig.tucuman.gov.ar/leyes/scan/scan/L-0-06062006.pdf (último ingreso el 12/3/2012).

b) Mientras la Constitución Argentina expresa que esta acción tiene por objeto tomar conocimiento de los datos referidos al titular y su finalidad, la Constitución de la Provincia de Tucumán amplía el objeto para incluir a sus bienes: "Toda persona podrá interponer acción expedita de *Habeas Data* para tomar conocimiento de los datos referidos a ella o a sus bienes y su finalidad".

c) Mientras la Constitución Argentina expresa que el sujeto pasivo de la acción de habeas data son los bancos de datos públicos o privados destinados a proveer informes; la Constitución de la Provincia de Tucumán en forma acertada evita hacer referencia al destino de los bancos de datos públicos o privados. Concretamente la diferencia está en que la Constitución de la Provincia de Tucumán no exige que deban ser bancos de datos destinados a proveer informes. Esta diferencia es una avance o evolución del instituto constitucional tucumano con respecto a la Carta Magna nacional porque conlleva una ampliación del alcance del habeas data sobre los sujetos pasivos de la acción, a todo tipo de bancos de datos, tanto públicos como privados y no se limita, como lo hace el texto de la Constitución Nacional, a los destinados a proveer informes. En la práctica la jurisprudencia ha corregido esta restricción poco feliz de la Constitución Nacional, al considerar que todo reflejo de datos personales que realice un banco de datos público o privados, aun cuando su actividad no sea dar informes, es un informe.

Consideramos esta diferencia un avance del instituto del *Habeas Data* porque los bancos de datos demandados usaban esta frase poco feliz de la Constitución Nacional, para plantear la falta de legitimación pasiva, por no ser "un banco de datos destinado a proveer informes". Este problema de redacción existente en la Carta Magna nacional, fue corregido en el texto de la Constitución de la Provincia de Tucumán.

d) También el texto de la Constitución de la Provincia de Tucumán amplia la descripción de los datos personales, a los falsos, erróneos, obsoletos, incompletos o de carácter discriminatorio, que darán lugar al

habeas data cancelatorio, rectificativo, actualizativo, aditivo o de actualización.

La tardía llegada del habeas data a la Constitución de la Provincia de Tucumán, doce años después de su incorporación a la Constitución Nacional, debería haber puesto a la Provincia de Tucumán en el escalón más alto del derecho público provincial. Podría haberlo logrado si hubiera incorporado una autoridad de control provincial en materia de protección de datos personales, de rango constitucional (como lo hizo con el Tribunal de Cuentas de la Provincia), autónoma, independiente y con presupuesto propio acorde a sus misiones y funciones.

Conjugando mi condición de abogado del foro tucumano al tiempo de preparar la presente tesis en la materia, he participado en algunos casos en los que actué como apoderado de la parte actora en amparos informáticos o habeas data. Uno de estos pleitos fue el caso "Núñez, Roberto c/ Nuevo Banco del Suquía S.A. s/ amparo informático" sustanciado en el año 2004 (antes de la reforma de la Constitución de la Provincia de Tucumán), en el Juzgado Civil y Comercial Común de la III Nominación de los Tribunales de la Ciudad de San Miguel de Tucumán, a cargo del Dr. Aráoz. La sentencia favoreció a Roberto Núñez, haciendo lugar a la acción de *Habeas Data* interpuesta. Posteriormente se planteó una demanda por daños y perjuicios en contra del Nuevo Banco del Suquía S.A., juicio en el que se llegó a un acuerdo indemnizatorio a favor de Roberto Núñez.

La novedad más reciente en materia de derecho a la autodeterminación informativa es la evolución del fenómeno de las Redes Sociales, que también ha comenzado a mostrar los patentes efectos perjudiciales para la intimidad y la autodeterminación informativa de las personas.

Las redes sociales son estructuras compuestas de grupos de personas, las cuales están conectadas por uno o varios tipos de relaciones, tales como amistad,

parentesco, intereses comunes o que comparten conocimientos. El concepto está basado en la idea de que el número de conocidos crece exponencialmente con el número de enlaces en la cadena, y sólo un pequeño número de enlaces son necesarios para que el conjunto de conocidos se convierta en la población humana entera. La teoría de las redes sociales no es un concepto nuevo y en ella han aportado sus ideas diferentes científicos, antropólogos, matemáticos e incluso el célebre sociólogo Émile Durkheim[608]. El software germinal de las redes sociales parte de la teoría de los Seis Grados de Separación, según la cual toda la gente del planeta está conectada a través de no más de seis personas, pero que al relacionar a esas personas con sus grupos de amistades y contactos, la red puede ir creciendo exponencialmente y alcanzar a prácticamente todas las personas del planeta.

Actualmente Facebook ya ha superado los 500 millones de usuarios y crece a una velocidad superior a 50 usuarios por minuto, motivos por los cuales se ha transformado en uno de los grandes fenómenos de nuestro tiempo.

Esta breve síntesis sobre las redes sociales da cuenta de la potencialidad del daño que puede ser causado a los datos personales, a su intimidad, a sus posibilidades de auto-determinarse informativamente, a su honor, a su honra y a su buen nombre, al cual se encuentra sometido mi mandante, siendo víctima de un premeditado acto de suplantación de la personalidad y de la identidad, conducta tipificada penalmente en diferentes sistemas jurídicos del derecho comparado. El delito o ilícito de "suplantación de la personalidad o de la identidad", puede darse en la conocida Red Social Facebook, y la vía procesal para ejercer los derechos garantías derivados de la protección de datos personales, puede ser planteada como una acción autosatisfactiva contra la red social.

[608] Émile Durkheim (Épinal, Francia, 15 de abril 1858 – París, 15 de noviembre 1917), sociólogo francés que estableció formalmente la sociología como disciplina académica. Junto con Karl Marx y Max Weber, es considerado uno de los fundadores de la sociología.

CAPÍTULO V: CONCLUSIONES

1.- Problema

1.1.- Tecnología y procesamiento de datos

Las tecnologías de la información y de las comunicaciones han demostrado ser aptas para el procesamiento y tratamiento de grandes volúmenes de información. Actualmente la transmisión de datos e informaciones constituye un proceso básico para la organización socioeconómica en un mundo globalizado donde las redes de comunicación no respetan las fronteras geopolíticas de los Estados. Por este motivo, las denominadas TIC, además de ser herramientas para el desarrollo social y económico, son también un ámbito de necesaria regulación para el derecho.

Los constantes avances de la electrónica, de la informática y de las telecomunicaciones durante todo el siglo XX y lo que va del actual, muestran un proceso histórico de evolución tecnológica al parecer incesante. Sin embargo, los efectos del tratamiento informático y telemático de los datos de carácter personal, sin control de la persona a quién pertenecen, afectan perjudicialmente en su privacidad e intimidad. Es evidente que toda persona necesita de una zona de reserva de su intimidad para alcanzar un desarrollo integral de su personalidad.

Esta penetración de las TIC en la intimidad de las personas nos enfrenta a un nuevo problema ético y jurídico. El poder sin límites de saber sobre los individuos permite tanto al Estado como al sector privado acumular y procesar datos personales para hacer, en algunos casos, un ejercicio abusivo e incluso un ilegal control social sobre los seres humanos. Ello implica una patente violación a los derechos y a las libertades fundamentales de las personas.

Cierto es que los Estados, las instituciones y las diferentes organizaciones del mundo contemporáneo necesitan de las modernas tecnologías informáticas y de las redes de comunicación para adquirir, valorar y clasificar la información. Con ella se toman decisiones orientadas a los fines y objetivos del bienestar general para

los cuales fue creado el Estado. Pero también es cierto que estas tecnologías son capaces de interconectar diferentes archivos de datos y obtener de ellos un detallado perfil de las personas, instrumento que sirve a quién tiene el poder de usarlo, tanto en el sector público como en el privado.

Ante este problema, la humanidad se encuentra ante el desafío de buscarle solución, y para ello ha optado por establecer una regulación normativa protectora de las personas en su derecho a la autodeterminación informativa y a la protección de los datos personales. El fundamento de estas normas se explica en la necesidad del sistema jurídico de poner límites a la acumulación y procesamiento de datos personales para que sus abusos no dañen nuestro derecho a la intimidad y a la autodeterminación informativa.

En este escenario la protección de datos se constituye en un elemento central de todo ordenamiento jurídico. Forma parte esencial del conjunto de los derechos constitucionales, a la vez que tiene una directa relación con la persona, sin distinción de nacionalidad o clase social.

Pero, desde la perspectiva jurídica la protección de datos presenta un volumen de casuística impropio para las áreas del conocimiento del derecho. La terminología técnica, el complejo funcionamiento de la electrónica y la dinámica evolutiva de la informática, potenciada por las telecomunicaciones, hace de esta área un lugar incómodo para los juristas. A ello hay que añadir una vertiginosa necesidad de adaptación legal a la constante evolución de las TIC.

1.2.- Uso masivo de las TIC

También podemos observar que el uso masivo de las TIC atraviesa todo tipo de culturas, religiones o geografías. En particular ha penetrado profundamente en la vida de las personas más jóvenes. Esto hace del derecho a la autodeterminación informativa una necesidad para garantizar la libertad, la dignidad, la igualdad y en particular el desarrollo integral de las personas.

Hemos aceptado que el fenómeno de la invasión en la intimidad y en la privacidad de los seres humanos es una consecuencia negativa de la sociedad de la información. También hemos comprendido que el derecho debe hacer su trabajo para proteger a las personas, y esto ha llevado a muchos países a dictar una legislación específica en la materia.

Sin embargo, también estamos comenzando a tomar conciencia que sólo con legislar no alcanza; se hace necesario que el Estado acompañe la legislación con políticas públicas que incluyan un conjunto de acciones y estrategias para alcanzar una protección real al derecho a la autodeterminación informativa.

Estas políticas deben pensar en proteger a personas que forman parte de un mundo globalizado, comunicado e informatizado. Debe pensar en personas propietarias del derecho a la autodeterminación informativa y como tal, en sujetos activos y titulares del derecho a proteger sus datos personales.

La carencia de políticas de Estado que incorporen componentes de las TIC dentro de sus programas de desarrollo, en un marco de evolución de la sociedad de la información, dejan tanto a la normativa que atañe al derecho de acceso a la información, como a la que se refiere a la protección de la intimidad, aisladas y muchas veces inaplicables.

Como agravante, se observa la falta de coordinación de esfuerzos a nivel subregional, regional e internacional, necesarios, como consecuencia de las características transfronterizas de los fenómenos de la sociedad de la información.

1.3.- Efectos de la conducta de las personas en el mundo virtual

Los problemas mencionados en los puntos anteriores nos permiten afirmar que las TIC ya forman parte de la vida cotidiana en nuestra sociedad, que su uso es masivo y que las nuevas generaciones, en particular, las han adoptado como una forma de vivir y de relacionarse con el resto de la comunidad.

Esta realidad interpela al derecho a una nueva interpretación jurídica de los efectos de la conducta de las personas en el mundo virtual. La ciencia jurídica debe definir si el uso constante de las redes de información, aportando datos personales, debilita el derecho a la autodeterminación informativa del titular de esos datos.

El mundo ha cambiado y cada día se hace más común y natural gestionar la vida en comunidad por medio de sistemas de gobierno electrónico, de educación virtual o de comercio electrónico. Pensemos en los sistemas de *home banking*, en la contratación de transporte aéreo, en la compra de libros o en el pago de impuestos por Internet. Los niños y los jóvenes de las nuevas generaciones nacieron rodeados de tecnología, y muchos directamente desconocen otras formas de realizar determinadas acciones que no sean en la modalidad del mundo virtual. A modo de ejemplo podemos pensar a un adolescente de nuestro tiempo, enviando un mail como algo muy natural y luego enviando una carta en el correo postal, introduciéndola en un buzón, como algo muy extraño.

Es pública y notoria la forma en que el uso masivo de la tecnología ha penetrado en la sociedad y en la vida diaria de las personas absorbiendo en forma compulsiva y voraz sus datos personales. Pertenecemos a una civilización que constantemente evoluciona tecnológicamente en el tratamiento de la información. La mayoría de las personas desconocemos sus efectos y los peligros a los que quedan expuestas al proporcionar, muchas veces con inocencia, sus datos personales.

Normalmente, sin darnos cuenta, propiciamos la vulneración de nuestro más sensible derecho a la intimidad y a la autodeterminación informativa. La educación y esencialmente las escuelas todavía no llegaron a comprender lo que ocurre en la sociedad de la información, y aún más, los diseños curriculares están profundamente desactualizados con respecto a los cambios que genera la tecnología. La escuela, generalmente conservadora, no cumple la función de preparar al individuo para su protección. Sus programas deberían preparar a los alumnos para

usar las redes de información sin exponerse a la vulneración de sus derechos a la autodeterminación informativa.

1.4.- Las Redes Sociales

Lo expresado en los puntos anteriores puede comprobarse en el crecimiento de las redes sociales. Ellas son un nuevo problema para la autodeterminación informativa por la gran penetración que han alcanzado en la sociedad.

Facebook ha superado los quinientos millones de usuarios[609] y a esta red social hay que sumar muchas otras. La potencialidad del daño que pueden causar a la autodeterminación informativa, puede llegar incluso a la suplantación de la personalidad y de la identidad de una persona.

Por este motivo es una nueva amenaza para la autodeterminación informativa de las personas. El derecho no debe desatender este problema y para ello debe pensar en forma anticipada en regular a las redes sociales, de manera tal que su uso siga creciendo, pero sin vulnerar los derechos fundamentales en general y en particular al derecho a la protección de los datos personales.

[609] Las redes sociales son estructuras compuestas de grupos de personas, las cuales están conectadas por uno o varios tipos de relaciones, tales como amistad, parentesco, intereses comunes o que comparten conocimientos. El concepto está basado en la idea que el número de conocidos crece exponencialmente con el número de enlaces en la cadena, y sólo un pequeño número de enlaces son necesarios para que el conjunto de conocidos se convierta en la población humana entera. La teoría de las redes sociales no es un concepto nuevo y en ella han aportado sus ideas diferentes científicos, antropólogos, matemáticos e incluso el célebre sociólogo Émile Durkheim. El software germinal de las redes sociales parte de la teoría de los Seis Grados de Separación, según la cual toda la gente del planeta está conectada a través de no más de seis personas, pero que al relacionar a esas personas con sus grupos de amistades y contactos, la red puede ir creciendo exponencialmente y alcanzar a prácticamente a todas las personas del planeta. Actualmente Facebook ya ha superado los 500 millones de usuarios y crece a una velocidad superior a 50 usuarios por minutos, motivos por los cuales se ha transformado en uno de los grandes fenómenos de nuestro tiempo.

2.- Recolección de Datos

2.1.- Utilidad del método comparativo

En el punto anterior, al describir el problema sobre el que trata esta tesis, observamos que la autodeterminación informativa se encuentra amenazada o bien directamente lesionada por las TIC. En otras palabras hemos comprobado la hipótesis planteada en el capítulo I, según la cual es necesario legislar sobre la protección de los datos personales para proteger a las personas en el ejercicio de su derecho a la autodeterminación informativa.

Para pensar en una legislación protectora de los datos personales, la comparación de las regulaciones nacionales existentes en Europa y América (con especial análisis de las legislaciones de España y Argentina), es sumamente útil en una materia tan técnica como esta.

El método comparativo, basado en la hermenéutica analógica, nos permite observar las carencias o los aciertos de las diferentes legislaciones vigentes en Europa y en América. Por medio de este método se visualizan mejor los problemas jurídicos y se aprecia con nitidez como diferentes normas que buscan regular una determinada conducta, pueden según su texto, alcanzar distintas situaciones de hecho.

El objetivo que nos planteamos en esta investigación es comparar el derecho a la protección de datos personales en Europa y América con especial análisis de las legislaciones de España y Argentina. Para ello, hemos comenzado con el objeto de estas normas y llegamos al estudio del concepto de intimidad y su diferencia con otros conceptos análogos. Luego analizamos la evolución histórica que acompaña al derecho a la intimidad y sus efectos sobre el nacimiento del nuevo derecho a la autodeterminación informativa, también llamado derecho de protección de los datos personales.

Una vez enfocado en este nuevo derecho a la autodeterminación informativa o de la protección de datos personales estudiamos primero el reconocimiento internacional alcanzado (OCDE y Consejo de Europa). Luego seguimos con la interpretación realizada por la jurisprudencia, en particular la alemana y española, sobre su alcance, su operatividad, su autonomía y las técnicas legislativas aplicadas en el derecho comparado para su regulación.

2.2.- Legislación de protección de datos personales

La hipótesis que justifica esta tesis postula que la solución planteada por el derecho para evitar los efectos perjudiciales del procesamiento informático y telemático de la información personal, en la intimidad de las personas, es la promulgación de leyes de protección de datos personales. Quedó demostrado en los capítulos segundo, tercero y cuarto, que los sistemas jurídicos de Europa y América han legislado en materia de protección de datos personales.

Cierto es que encontramos diferentes sistemas de legislación de protección de datos personales, algunos sólo enuncian una normativa escueta, otros una más completa. Algunas de estas leyes determinan un proceso judicial de tutela concreto y le asignan la función de control a una autoridad de aplicación independiente con recursos humanos y materiales suficientes para velar por el respeto a los derechos relacionados con la intimidad, la identidad y la autodeterminación informativa de las personas.

Los sistemas normativos de protección de datos personales vigentes en Europa son la consecuencia de un largo proceso evolutivo que comienza con una primera generación de leyes de protección de datos personales surgida en la década de 1970.

Desde esa primera generación normativa de la década del 70, pensada para limitar la utilización de las nuevas tecnologías de la información mediante la reglamentación del funcionamiento de los bancos de datos, a nuestros tiempos, donde los equipos informáticos son cada vez de menor tamaño físico, de mayor

capacidad de memoria, de mayor versatilidad y velocidad, el derecho ha tenido que adaptarse a estos constantes cambios tecnológicos para idear un sistema jurídico más justo y eficaz que acompañe la evolución tecnológica.

La mencionada primera generación de leyes de protección de datos personales fue sancionada para un mundo donde los bancos de datos pertenecían en su gran mayoría al sector público, eran pocos, ocupaban grandes espacios físicos, tenían escasa memoria, contaban con baja capacidad de procesamiento y prácticamente nula compatibilidad y posibilidades de conexión.

Sin embargo, los descubrimientos realizados en el campo de la microelectrónica hicieron necesaria una nueva generación de leyes de protección de datos orientada a las nuevas posibilidades de creación de bancos de datos en espacios físicos más reducidos, más versátiles y con un menor costo. Así, surgieron las leyes de segunda generación con la consigna de asegurar la calidad de los datos, dar protección a la información sensible de las personas y garantizar el derecho de acceso y control de las informaciones personales por parte de los titulares de los datos. El legislador dictó nuevas normas para regular una sociedad donde se había generalizado el uso de bancos de datos, tanto en el sector público como en el sector privado.

Pero el proceso de evolución normativa en la materia no se cerró y en la década de 1980, las leyes de protección de datos nuevamente recibieron el impacto de los cambios tecnológicos. Esta vez impulsados por la revolución de las telecomunicaciones.

También en este tiempo se promulgó en 1981 el Convenio 108 del Consejo de Europa para la Protección de los Datos Personales, considerado como una de las primeras normas surgidas en la tercera generación de leyes de protección de datos personales.

Más tarde llegará la Ley de Protección de Datos de Gran Bretaña en 1984 (*The Data Protection Act*), la Directiva de la Unión Europea 95/46/CE y la Ley

Orgánica española nº 5/92 (conocida como la LORTAD, hoy derogada por la LOPD), de regulación del tratamiento automatizado de datos, entre otras normas.

La promulgación y vigencia de las mencionadas normas, junto a la jurisprudencia europea en materia de protección de datos personales ejerció influencia en el continente americano, a tal punto que se reformaron muchas constituciones para incluir en su texto el derecho garantía de *habeas data*.

2.3.- La jurisprudencia

La jurisprudencia también fue acompañando al proceso evolutivo de las normas de protección de datos personales, por medio de su interpretación del derecho a la intimidad.

En el año 1983 el Tribunal Constitucional Federal alemán declaro parcialmente inconstitucional la ley alemana del censo del 4 de marzo de 1982. En este fallo podemos encontrar el principal fundamento del tránsito entre las leyes de protección de datos de 2ª generación que fueron evolucionando hacia las de 3ª generación. La sentencia del tribunal alemán señala que la proliferación de centros o bancos de datos permite producir una imagen pormenorizada, que constituye una seria amenaza para la intimidad, para la autodeterminación informativa y para la dignidad de las personas.

Con esta sentencia se abrió paso una tercera generación de leyes de protección de datos personales que llegó con la consigna de adaptar la legislación a la vertiginosa evolución que la microinformática y las redes de comunicaciones telemáticas exigían al derecho como sistema de protección de las personas pensado para un mundo con bancos de datos interconectados con redes y puntos de información distribuida que han sustituido a los antiguos y voluminosos centros de cómputos. Las leyes protección de datos personales, pertenecientes a la tercera generación, impulsadas por la sentencia de Tribunal Constitucional alemán, surgen en un contexto en el que las computadoras personales son más pequeñas, más compactas y de fácil conexión a las redes de comunicación.

2.4.- Legislación Europea

En el derecho comparado analizamos normas que regulan el derecho a la protección de datos personales en la Unión Europea (por medio de resoluciones y directivas) y en sus Estados miembros. España, Alemania, Austria, Bélgica, Dinamarca, Francia, Grecia, Holanda, Irlanda, Italia, Portugal, Reino Unido, Suecia y Noruega, entre otros Estados, han legislado en la materia.

En estos países (todos miembros de la Unión Europea) se observa una legislación homogeneizada por las directivas europeas que expresa un derecho a la protección de datos personales consolidado. Esta legislación también contempla principios de protección de datos, un proceso de reclamación claro, órganos de aplicación independientes del Poder Ejecutivo y normas expresas de transferencia internacional de datos. La Unión Europea sigue avanzando en el proceso de consolidación de una normativa aún más homogénea. La Comisión Europea ha presentado en el año 2012 el Proyecto de Reglamento Europeo de Protección de Datos Personales, con el objetivo de uniformar la normativa del espacio común europeo en la materia.

2.5.- Legislación americana

En el continente americano encontramos una realidad diferente. Mientras América del Norte ha legislado en la materia en la década de 1980, el resto del continente recién comenzó más tarde un proceso de incorporación de normas de protección de datos personales que todavía no ha concluido. Encontramos un estado de evolución normativa, todavía abierto, de incorporación de cláusulas constitucionales en la mayoría de los Estados de Centro América y de Sudamérica.

La mayoría de las constituciones americanas han comenzado por adoptar cláusulas constitucionales protectoras de los datos personales con la forma de una

acción de amparo, es decir una acción constitucional directa de garantía que se conoce con el nombre de *habeas data.*

En algunos de estos países (no todos) también existen normas que desarrollan las mencionadas clausulas constitucionales de *habeas data*, pero el problema que encontramos es que esas legislaciones no son homogéneas entre ellas y por lo tanto insuficientes para proteger a las personas en un mundo globalizado e intercomunicado. En la mayoría de los casos no cuentan con un órgano de aplicación y los pocos Estados que los han creado, no le dieron autonomía ni independencia del Poder Ejecutivo.

Nuestro estudio observó las legislaciones del MERCOSUR, Argentina, Estados Unidos, Bolivia, Brasil, Perú, Nicaragua, Panamá, Canadá , Colombia, Chile, Costa Rica, Ecuador, México, Paraguay, Uruguay, Venezuela y El Salvador. En ninguna de estas legislaciones el legislador ha contemplado la existencia de un órgano o autoridad de control independiente del Poder Ejecutivo.

Ya hemos visto cómo los permanentes cambios tecnológicos requieren que leyes de protección de datos personales tengan un contenido evolutivo que procure la adaptación de la ley a los avances de la informática y de las telecomunicaciones.

Las conductas humanas agresivas a la intimidad y cuestiones tales como los números de identificación única (por ejemplo el CUIT o el CUIL en Argentina), las investigaciones sobre el genoma humano o la tele vigilancia, nos llevan a reflexionar sobre la necesidad de incorporar nuevas leyes de protección de datos personales que regulen y limiten los desarrollos científicos que acumulen datos genéticos de las personas en forma injustificada y sin control del Estado.

La incorporación de garantías constitucionales y la promulgación de leyes de protección de los datos de carácter personal es sólo un primer paso para lograr una efectiva protección jurídica de la autodeterminación informativa de las personas. No olvidemos que en contraposición al derecho a la protección de los datos personales, se encuentra el derecho humano de tercera generación a la información, también

protegido en las diferentes constituciones de los Estados y por pactos internacionales. Un equilibrio entre ambos derechos es un complejo desafío jurídico de nuestra sociedad contemporánea. Ambos derechos surgen de una necesidad humana, ambos son derechos fundamentales, ambos son derechos humanos y en muchos Estados también son derechos constitucionales.

Las leyes de diferentes estados del mundo protegen el derecho a la intimidad en forma genérica, pero para proteger seriamente el derecho a la autodeterminación informativa de las personas, es necesario una norma constitucional expresa que proteja los datos personales junto a una ley de protección de datos de carácter personal que desarrolle el precepto constitucional, determine un procedimiento concreto con reglas procesales claras y proceda a la creación de un órgano de aplicación y control apto para velar por el cumplimiento de la ley. La enunciación de los derechos o garantías constitucionales debe ir acompañada de la determinación de un debido proceso, claro y concreto. Son muchos los derechos y libertades que enumeran las Constituciones, pero no así los mecanismos reales con los que aquellos se pueden proteger efectivamente.

2.6.- La protección de datos personales en Argentina

Al realizar un análisis particular de la situación Argentina encontramos que su Constitución incorporó con la reforma del año 1994 una nueva garantía constitucional para proteger los datos personales. Luego, a fines del año 2000 entró en vigencia la ley Nº 25.326, de protección de datos personales, con el objeto de desarrollar legislativamente la garantía constitucional de *habeas data*, incorporada en el artículo 43, tercer párrafo, de su Constitución.

La ley de protección de datos de la República Argentina aún no ha logrado gran eficacia en la protección de los datos personales. La creación de un órgano de control (la Dirección Nacional de Protección de Datos Personales) dirigido por un funcionario dependiente del poder Ejecutivo y con escasos recursos, ha limitado las

buenas intenciones manifestadas por el legislador argentino al momento de su debate parlamentario.

Las funciones y atribuciones otorgadas al órgano de control por la ley 25.326 con la obligación legal de realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones legales no han sido efectivas. Han pasado más de doce años desde la promulgación de la ley 25.326 y todavía no ha logrado avances concretos.

Como ya dijimos, la ausencia de un órgano de control independiente del Poder Ejecutivo ha frustrado las intenciones y el espíritu de la ley argentina 25.326. Pero cabe aclarar que el proyecto de ley sancionado por el Congreso de la Nación, había diseñado un órgano de control dotado de autonomía funcional. Sin embargo, el Poder Ejecutivo Nacional, a través del Decreto 995/2000, vetó los incisos 2º y 3º del artículo 29 de la ley, eliminando todo tipo de independencia del órgano de control. El vetado inciso 3º del artículo 29 expresaba que la administración y dirección del órgano de control recaía en un Director seleccionado entre personas con antecedentes en la materia, y designado por el término de cuatro años por el Poder Ejecutivo Nacional, con acuerdo del Senado de la Nación.

Con el veto realizado por el presidente Fernando De la Rúa, en el año 2000, al inciso 3° del art. 29 de la ley 25.326, se transformaron en ilusorias todas las posibilidades de eficacia preventiva de la ley de protección de los datos de carácter personal, porque al quedar facultado al Poder Ejecutivo de la Nación para designar al Director del órgano de aplicación de la ley sin control del Congreso de la Nación sus posibilidades de actuar quedaron muy reducidas.

El veto, mencionado en el párrafo anterior, dejó en la ley un vacío legal que repercute en la regulación de la autoridad de control. A modo de ejemplo, nada quedó legislado sobre el tiempo mínimo de permanencia del Director en sus funciones.

El veto parcial del Poder Ejecutivo a la ley de protección de datos personales generó que la Dirección Nacional de Protección de datos quedara en una situación de absoluta debilidad y dependencia del gobierno de turno.

A ello se suma, como dato agravante, que la mayor acumulación de datos personales en Argentina, la realizan los organismos centralizados y descentralizados de la administración pública del Estado.

Sin embargo, a diferencia de lo sucedido en Argentina, la mayor parte del derecho comparado europeo ha buscado fortalecer la independencia de las autoridades de control para dotar de mayor eficacia a la legislación de protección de los datos de carácter personal. A modo de ejemplo podemos mencionar a España.

La defensa de los derechos de los afectados, así como la garantía de que la ley se va a aplicar correctamente, exige la presencia de un organismo de control independiente que vele por que esto así ocurra. La ley española hace hincapié, en su artículo 35º, en el carácter independiente del órgano de control y de su Director, a quien le garantiza un tiempo fijo de mandato, que solo puede ser acortado por un número taxativo de graves causas de cese.

Tratamos en el capítulo anterior de esta tesis, la protección de los datos de carácter personal en las provincias argentinas. Observamos en ellas la falta de un órgano de control provincial, motivo por el cual muchas personas quedan desprotegidas frente a la acumulación y procesamiento de sus datos personales.

En el territorio amplio y descentralizado de un país federal como Argentina, es necesaria la creación de órganos de control locales especializados en protección de los datos de carácter personal. Generalmente el argumento político para rechazar la creación de una autoridad de protección de datos personales es la falta de presupuesto. Ante este argumento se puede proponer como solución momentánea, hasta tanto se resuelva el problema presupuestario, dotar de competencias y jurisdicción en la materia al Defensor del Pueblo. Esto es posible toda vez que las

provincias argentinas cuentan con defensorías del pueblo autónomas e independientes del Poder Ejecutivo provincial.

Si comparamos el derecho español de protección de datos personales, con el argentino, encontramos que ambos han recorrido un proceso de evolución. Tenemos evidencia de la declaración del derecho a la protección de los datos personales en toda Europa, en casi toda América y en diferentes lugares del mundo.

Sin embargo, no podemos decir lo mismo del aprendizaje o conciencia de las personas que viven en estos Estados sobre el derecho que les cabe a proteger sus datos personales y mucho menos podemos hablar de una apropiación de este derecho. Los países o Estados cuyos ciudadanos tienen un mayor conocimiento, aprendizaje y apropiación del derecho a la protección de sus datos personales, son aquellos en los cuales se observa un mayor compromiso estatal en la difusión de este derecho, en la información y en el fomento al control de cada persona sobre sus datos personales. También es necesario para alcanzar una protección de datos personales real, el funcionamiento de un sistema de reclamación judicial y extrajudicial simple, rápido y operativo.

Los datos recolectados en los capítulos precedentes nos muestran que las constituciones políticas de los Estados analizadas, consagran derechos y libertades fundamentales para garantizar que cada persona pueda pensar, expresar y obrar, siendo la libertad de los otros el único límite de la libertad de cada uno.

Por ello al derecho a la protección de los datos de carácter personal, podemos considerarlo como un derecho humano de tercera generación, consagrado y garantizado entre los derechos fundamentales de las constituciones de América y Europa. El derecho a la protección de los datos personales, en tanto especie autónoma del género derecho a la intimidad, procura el respeto por la dignidad de las personas, buscando generar las condiciones necesarias para el desarrollo integral de la personalidad en el contexto de nuestra sociedad tecnológicamente desarrollada.

Cierto es que los derechos pueden ser declarados por una constitución o por una norma determinada, pero desde la declaración de un derecho hasta su aprendizaje y apropiación hay un largo camino evolutivo, en el cual el Estado tiene una importante responsabilidad.

3.- Resultados

La comparación de las leyes vigentes en Europa y América, junto con el estudio y análisis de la doctrina y jurisprudencia más relevante en materia de derecho a la protección de datos personales, nos ha permitido llegar a las siguientes conclusiones y propuestas:

Primera conclusión

Para disminuir la lesión al derecho a la intimidad y a la autodeterminación informativa provocada por el procesamiento automatizado de datos personales es necesario desarrollar una legislación específica de protección de datos personales con alcance global, que establezca un procedimiento de acceso y rectificación claro junto al control de una autoridad de aplicación especializada, independiente y autónoma del Poder Ejecutivo del Estado.

Segunda conclusión

Para lograr eficacia en la aplicación de la legislación en materia de protección de datos personales es necesario contemplar las siguientes cuestiones que sintetizamos en los siguientes puntos:

1.- Determinar un proceso judicial de tutela al derecho a la protección de datos personales claro y concreto

2.- Asignar la función de control a una autoridad de aplicación independiente, dotada de recursos humanos y materiales suficientes para velar por el respeto a los derechos a la autodeterminación informativa de las personas.

La experiencia internacional aconseja la existencia de una autoridad de aplicación en la materia, que cuente con independencia y autonomía. La inexistencia o debilidad de la autoridad de control redunda en una excesiva judicialización de los procedimientos de *habeas data*. Observamos que cuando las personas no cuentan con una protección jurídica de los datos personales organizada por la administración pública y tutelada por una autoridad de control independiente, judicializan sus reclamos. Algunas veces estos procesos judiciales se plantean sólo para obtener el acceso a los datos personales que conciernen al titular de esa información.

No ocurre lo mismo en aquellos Estados que cuentan con una autoridad de control fuerte e independiente y un procedimiento de reclamación claro, que se sustancia en forma extrajudicial ante el organismo de control. La judicialización del reclamo se transforma en una excepción, y de esta forma se evitan litigios judiciales que generan costos y desgaste para la administración de justicia.

La autoridad de control, independiente y autónoma del Poder Ejecutivo tiene que contar con jurisdicción, recursos y facultades para inspeccionar y sancionar, cuando así corresponda, a registros, bancos o bases de datos públicos o privados.

3.- Establecer que el órgano de control realice campañas públicas de concientización al ciudadano sobre la necesidad de dar protección a sus datos personales mediante el ejercicio derecho a la protección de sus datos personales. Los países o Estados cuyos ciudadanos tienen un mayor conocimiento, aprendizaje y apropiación del derecho a la protección de sus datos personales, son aquellos en los cuales se observa un mayor compromiso estatal en la difusión de este derecho, en la información y en el fomento al control de cada persona sobre sus datos personales.

Sólo con legislar no alcanza. Es necesario que el Estado acompañe la legislación con políticas públicas que incluyan un conjunto de acciones y estrategias

para alcanzar una protección real al derecho a la autodeterminación informativa de las personas.

Estas políticas deben pensar en proteger a personas que forman parte de un mundo globalizado, comunicado e informatizado; personas propietarias del derecho a la autodeterminación informativa y como tal, sujetos activos y titulares del derecho a proteger sus datos personales. En consecuencia la legislación, que se dicte al efecto, debe tender a un alcance global o por lo menos regional y con un contenido que además de sancionador sea reparador y mucho más preventivo.

4.- Adecuar en forma periódica las normas de protección de datos personales a la evolución de la tecnología. El alcance y la penetración global de las TIC, requiere de la necesaria adecuación que preste atención a los descubrimientos y a las innovaciones que presente la ciencia y la tecnología.

5.- Respetar los tratados internacionales que consideran al derecho a la autodeterminación informativa y a la protección de datos personales como un derecho humano, que no puede ser excluido, desconocido o restringido.

6.- Armonizar la legislación, de forma tal que su regulación garantice un alcance regional e internacional, que contrarreste el desarrollo global de las redes de comunicación. En tal sentido, la normativa debe fomentar acuerdos regionales y convenios internacionales que busquen la armonía de las normas de protección de datos personales[610].

La armonización normativa que proponemos debe intentar lograr una legislación cuyo contenido no sea prioritariamente sancionador o reparador, sino también de tipo preventivo (es decir, que promueva el empoderamiento de los sistemas de control con inspecciones, con capacitación y difusión pública de los peligros que asechan y de los derechos que tienen las personas). Esta legislación

[610] La ausencia de una legislación homogénea de alcance global en esta materia, debilita la protección que una región o Estado pueda dar a las personas y dificulta tanto la cooperación internacional como las relaciones económicas, empresariales, laborales, científicas que requieren de la transferencia internacional de datos para funcionar.

debe establecer acciones concretas que otorguen amplios derechos a las personas en su calidad de sujetos titulares del derecho a la intimidad y a la autodeterminación informativa. En otras palabras, pensar en una regulación de alcance amplio y dinámico que otorgue un rol protagónico al titular del derecho y no sólo un estatuto de carácter defensivo[611]. En esta línea se pronuncia el Proyecto de Reglamento de Protección de Datos del año 2012 presentado por la Comisión Europea (ver *ut supra*: Cap. II; 2.6.1.-).

7.- La protección de datos de las personas jurídicas debe alcanzar situaciones muy concretas, a los efectos de evitar el uso perverso del instituto para ocultar u opacar actividades ilícitas, prohibidas o no queridas por la ley, realizadas por este tipo de organizaciones.

8.-Las empresas de telecomunicaciones deben estar sujetas a controles especiales sobre los datos personales que recaban, procesan, almacenan y ceden a terceros.

9.- La conducta pasada de las personas en el mundo virtual no deben ser un fundamento para otorgar una mayor o menor protección a los datos personales de una persona determinada.

Rechazamos toda posibilidad de otorgar una mayor o menor protección o reparación al derecho a la autodeterminación informativa, bajo condición del análisis de los actos realizados dentro de las redes de información en el pasado[612]. En caso contrario, estaríamos legislando estatutos de derechos diferentes para cada persona y llegaríamos al absurdo de desarrollar un derecho con contenido cambiante

[611] A modo de ejemplo podemos mencionar que la vigente ley española (LOPD) otorga a las personas los derechos a la impugnación de valoraciones, consulta, acceso, rectificación y cancelación, oposición, tutela e indemnización. La LOPD contempla el derecho de oposición, que es el derecho que tienen los titulares, en determinadas circunstancias, a oponerse al tratamiento de los datos que les conciernen, caso en el cual, previa petición y de forma gratuita, serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud. El derecho de oposición de la LOPD española podría ser incorporado en las futuras reformas que se realicen en las leyes americanas.

[612] Contraria a esta posición, Herrán Ortiz (1999); op. cit. Acepta un condicionamiento mínimo de los actos propios y de los usos y costumbres en el alcance de la protección que se garantiza a cada individuo.

y diferente para la protección de los datos personales en función del sujeto respecto del cual se predique.

Tercera conclusión: propuestas para mejorar la legislación Argentina

La ley argentina Nº 25326 es un importante y auspicioso catálogo de derechos a la protección de los datos personales; sin embargo, es necesario reconocer sus debilidades y proyectar una reforma que busque superarlas.

Consideramos que los puntos débiles de esta ley son los siguientes:

1.- La excesiva debilidad y dependencia de la autoridad de aplicación, creada por la respecto del Poder Ejecutivo de la Nación. Esta falencia de la ley se agrava si consideramos que la Dirección Nacional de Protección de Datos Personales es el órgano regulador que tiene como principal objetivo proteger los datos de las personas físicas y jurídicas, almacenados en bancos de datos tanto privados como públicos, incluso los pertenecientes al Estado Nacional;

2.- La falta de una asignación presupuestaria otorgada a la Dirección Nacional de Protección de Datos Personales, para el cumplimiento de las misiones y funciones establecidas por la Ley 25.326 y sus decretos reglamentarios, conspira contra la existencia de controles reales y eficaces que se deben realizar a los bancos de datos, sean públicos o privados;

Proponemos como solución a este problema, la modificación de la Ley 25.326, a los efectos de otorgar independencia, autonomía y autarquía a la autoridad de control y aplicación. El presupuesto que se asigne a la Dirección Nacional de Protección de Datos Personales debe ser acorde a las necesidades que como autoridad de aplicación nacional, tiene para cumplir con las misiones y funciones asignadas por la ley 25.326 y sus normas reglamentarias en todo el territorio argentino.

3.- La protección a la intimidad de las personas ideales o jurídicas en un plano de igualdad con las personas físicas, dado que el trato igualitario a personas

físicas y jurídicas contradice el principio por el cual se exige publicidad y transparencia de los actos de las personas jurídicas o ideales. Proponemos la sanción de una ley específica que tenga por objeto la protección del derecho a la intimidad de las personas de existencia ideal.

4.- La ausencia de una regulación específica que proteja los datos personales acumulados por las empresas de telecomunicaciones sobre sus abonados. La gran cantidad de datos personales de sus abonados que procesan y acumulan las empresas de telecomunicaciones justifica una regulación diferenciada con sanciones agravadas para el incumplimiento de la normativa en materia de protección de datos personales. La regulación que se dicte al efecto debe establecer como límite de tiempo de conservación de datos los clientes, por parte de las empresas de telecomunicaciones, el plazo de tiempo en el cual la factura de consumo pueda ser recurrida.

5.- La ausencia de normas que obliguen al Poder Ejecutivo y al órgano de control a realizar campañas de difusión sobre el derecho a la protección de los datos personales y de concientización sobre el ejercicio del derecho a la autodeterminación informativa. La regulación normativa propuesta deberá establecer la obligación de la Dirección Nacional de Protección de Datos Personales, de realizar campañas públicas de difusión del derecho a la protección de datos personales y su ejercicio.

6.- La debilidad de un proceso de garantía a la protección de datos personales que otorga derechos defensivos y activos a las personas: de oposición, de impugnación a las valoraciones personales, de consulta, de acceso, de rectificación, de cancelación y de indemnización por violación a la autodeterminación informativa de la persona.

El proceso actual debe ser fortalecido y acompañado por acuerdos entre el Estado Nacional y las Provincias para su aplicación armónica en todo el territorio nacional.

Reflexión final

Estamos ante la necesidad de resolver un problema que afecta a la humanidad y al que el derecho debe dar respuesta. En este camino es importante recordar una vez más a Arnold Toynbee[613], cuando expresaba que "el grado de dominio que posee una sociedad sobre su contorno físico puede medirse por su técnica. Pero la técnica no es parámetro para medir el crecimiento de una sociedad o civilización, ya que el crecimiento consiste en el progreso hacia la autodeterminación y superación de obstáculos materiales que impiden que las energías de una sociedad den respuesta a incitaciones tanto internas como externas, espirituales antes que materiales". Pensamos que la conquista de la autodeterminación informativa es el gran desafío interno y espiritual que debe alcanzar nuestra generación.

[613] Toynbee, A. *Estudios de la Historia.* Compendio IX/XIII (Tomo 3). Sexta re-impresión. Editorial Alianza. Madrid, 1991, p. 339.

RECURSOS BIBLIOGRÁFICOS

Los recursos bibliográficos para realizar esta tesis se obtuvieron de los fondos bibliográficos de las bibliotecas del Congreso de la República Argentina, de la Facultad de Derecho de la Universidad Nacional de Tucumán, del Departamento de Filosofía, Moral y Política de la Facultad de Derecho de la Universidad Complutense de Madrid, de la Biblioteca Central de la Universidad Nacional de Tucumán (Argentina), de la Agencia de Protección de Datos Personales de España, de la Dirección Nacional de Protección de Datos de Argentina y de la biblioteca personal del director de tesis y del doctorando.

BIBLIOGRAFÍA

En orden alfabético:

Alderman, E.; Kennedy C. *The Right to Privacy*. Ed. Random House, New York(EEUU), 1997.

Basterra, M. I. *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01Comentados. Derecho Constitucional Provincial. Iberoamérica y México.* Editorial Ediar – Universidad Nacional Autónoma de México (UNAM). Buenos Aires/México D.F., 2008.

Basterra, M. *Derecho a la información vs. Derecho a la intimidad*. Ed. Rubinzal – Culzoni Editores. Santa Fe, 2012.

Botta, M. *Tesis, monografías e informes. Nuevas normas y técnicas de investigación y redacción*. Editorial Biblos. Buenos Aires, 2002.

Cabezuelo Arenas, A. *Derecho a la Intimidad*. Editorial Tirat lo Blanch, (Tirant, monografías n° 96), Valencia, 1998.

Castells, M. *La Era de la Información. Vol.1.Sociedad en Red*. (Trad. Carmen Martínez Gimeno y Jesús Alborés). 1ª reimpresión; 3ª ed. Alianza Editorial. Madrid, 2008.

Cattaruzza, A.; Galbiati, R.; Panieri, B., y Zampetti, A. *La tutela dei dati personali*. 2º ed. Editorial Buffetti Editori Multimedia. Grupo Buffetti. Roma, 1998.

Constitución Política de la República del Ecuador. Ley de Control Constitucional. Editorial Galbar, Quito (Ecuador), 2002.

Constitución Política de la República del Ecuador. Editorial EDIJUR, Quito (Ecuador), 2003.

Constitución de la República Bolivariana de Venezuela. 2ª ed., Editorial TEMIS S.A. Rincón. Bogotá, 2000.

Cuadernos de Debates Nº 21. Centro de Estudios Constitucionales (Madrid); 1989. Dentro de esta obra: Losano, M. *Los orígenes de la Data Protection Act inglesa de 1984*.

Código Civil y Comercial de la Nación. Proyecto del Poder Ejecutivo de la Nación redactado por la Comisión de Reformas designada por Decreto 191/2011. Presentación del Proyecto por Ricardo Luis Lorenzetti. Editorial Rubinzal – Culzoni, Santa Fe, 2012

Dalla Vía, A.; Basterra, M. I. *Habeas data y otras garantías constitucionales*. Editorial Némesis, Buenos Aires; 1999.

Davara Rodríguez, M. "La ley española de protección de datos (LORTAD): ¿una limitación al uso de la Informática para garantizar la intimidad?". Revista Actualidad Jurídica N° 76, Editorial Aranzadi, Pamplona, 12 de noviembre de 1992.

Davara Rodríguez, M. *La protección de Datos en Europa. Principios, Derechos y Procedimiento*. Editorial Grupo ASNEF EQUIFAX – Universidad Pontificia Comillas de Madrid – ICAI-ICADE. Madrid, 1998.

Del Peso Navarro, E.*Ley de protección de datos, la nueva LORTAD*. Editorial Díaz de Santos. Madrid, 2000.

Del Peso Navarro, E.; Ramos González, M. *Confidencialidad y Seguridad de la Información: La LORTAD y sus implicancias socioeconómicas*. Editorial Díaz de Santos. Madrid, 1994.

Delpiano A. "La protección de datos personales. Bancos de Datos de Información crediticia".Editorial Fcu, colección JVS, Nº 47. Montevideo, año 1997.

Denniger, E. *El derecho a la autodeterminación informativa*. Publicado en: *Problemas actuales de la documentación informática jurídica*. Ed.Tecnos. Madrid, 1987.

Diccionario de la Lengua Española. Real Academia Española. Editorial Espasa-Calpe. 21ª Edición (1992) y 22ª Edición. Madrid, 2006.

Diccionario de Latín Jurídico. *Locuciones latinas y su aplicación jurídica actual*. Autores: Washington Rodríguez, A.; Galeta de Rodríguez, B. Editorial García Alonso, Buenos Aires, 2006.

Drucker, P. *La sociedad poscapitalista*. Editorial Sudamericana. Barcelona, 1999.

Ekmekdijan. M.; Pizzolo Calogero (h). *Habeas data: El derecho a la intimidad frente a la revolución informática*. Editorial Depalma, Buenos Aires, 1996.

Falconi, J. *El Juicio Especial por la acción de habeas data; y los derechos constitucionales a: la intimidad; privacidad; imagen; al honor; a la no discriminación; a la igualdad; al de petición; al de información, sus limitaciones y responsabilidades*. Editorial Rodin. Quito (Ecuador), 2000.

Finnis, J. *Natural Law and Natural Rights*. 2ª ed. Editorial Oxford University Press. Nueva York, 2011.

Foucault, M. *Vigilar y Castigar. Nacimiento de la prisión*. 16ª reimpresión. (Primera edición en España: 1979). Editorial Siglo XXI Editores. Madrid, 2009.

Frixes San Juan, T. *Obtención y utilización de datos personales automatizados*. Publicado en Actas de las Jornadas sobre derecho español de la protección de datos.

Gozaíni, O. *Derecho Procesal Constitucional .Habeas Data. Protección de datos Personales. Doctrina y Jurisprudencia*. 1ª ed. Editorial Rubinzal – Culzoni Editores. Buenos Aires, 2001[614].

Gozaíni, O. *Derecho Procesal Constitucional. Habeas Data. Protección de datos Personales. Doctrina y Jurisprudencia*. 2ª ed. Editorial Rubinzal – Culzoni Editores. Santa Fe, 2011.

[614] La publicación de esta obra fue acompañada por un CD-ROM en el cual se encuentra el texto de la ley 78/17 traducido al castellano. ISBN: 950-727345.

Gozaíni, O. *Derecho Procesal Constitucional. Habeas Data. Protección de datos Personales. Ley y Reglamentación.* 1ª ed. Editorial Rubinzal –Culzoni Editores. Santa Fé, 2002.

Herrán Ortiz, A. *La violación de la intimidad en la protección de datos personales*. Editorial Dykinson. Madrid, 1998.

Hobbes, T. *Leviatán*. (Trad. de Antonio Escohotado). Editora Nacional de Madrid. Madrid, 1980.

Hubeñák, F. *Formación de la Cultura Occidental*. Editorial Ciudad Argentina. Buenos Aires, 1999.

Hubeñák, F. *Historia Integral de Occidente. Desde una perspectiva cristiana.* Editorial EDUCA. Buenos Aires, 2006.

Infantes Madujano, P. *Constitución Política del Perú*. Editorial Librería y Ediciones Jurídicas. Lima, 1999.

Iriarte Ahon, E. (Coordinador de Edición). *Informe de Análisis y Propuestas en Materia de Acceso a la Información y Privacidad en América Latina*. (Documento desarrollado dentro del Proyecto Monitor de Privacidad y Acceso a la Información en América Latina). Editado por UNESCO. Lima, 2007.

Presidencia del Gobierno. *Informática. Leyes de Protección de Datos (II)*. Documentación Informática N° 3. Serie Verde/ Legislación. Presidencia del Gobierno (España). Servicio Central de Publicaciones. Servicio Central de Informática. Ed. Imprenta Nacional del Boletín Oficial del Estado. 1ª ed. Abril de 1983. Madrid, 1983

Locke, J. *Carta sobre la Tolerancia*. Editorial Tecnos, (6ª Edición). Madrid, 2008.

Locke, J. *Ensayo sobre el gobierno civil*. Editorial Aguilar. Madrid, 1981.

Lozano, M.; Pérez Luño, A.; Guerrero Mateus, M. *Libertad informática y leyes de protección de datos personales.* Publicado en Cuadernos y Debates. Publicación del Centro de Estudios Políticos y Constitucionales de Madrid. Madrid, 1989.

Luna, F. *Breve Historia de los Argentinos*. Editorial Planeta Argentina. Buenos Aires, 2000.

Mac Nall Burns, E. *Civilizaciones de Occidente. Su historia y su cultura.* Ediciones Peuser, 3ª Edición. Buenos Aires, 1953.

Martín-Casallo López J. (Coord.) *El Consejo de Europa y la Protección de Datos Personales*. Editada por la Agencia de Protección de Datos. Editorial De Arellano. Madrid, 1997.

Mattelart, A. *Historia de la Sociedad de la Información.* (Trad. Gilles Multigner).1ª Ed. en la colección de bolsillo. Editorial Paidós. Madrid, 2007.

Mill J. *Sobre la Libertad*. (Trad. Cantera, G.). Editorial EDAF. Madrid, 2004.

Murillo de la Cueva, Lucas. *El derecho a la autodeterminación informativa*. Editorial Tecnos. Madrid, 1990.

Murillo de la Cueva, Pablo Lucas. *Informática y Protección de Datos Personales (Estudio sobre la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal).* Cuadernos y Debates N° 43. Centro de Estudios Constitucionales. Madrid, 1993.

Nora, S.; Minc, A. *La Informatización de la Sociedad: Informe al Presidente de la República*. Editorial Fondo de Cultura Económica. México, 1981.

Ortega y Gasset, J. *Meditación de la técnica*. Editorial Revista de Occidente, 3ª Edición en Castellano. Madrid, 1957.

Ortecho Villena, V. *Jurisdicción y Procesos Constitucionales*.7ª ed. Editorial Rodhas. Lima (Perú), 2002

Orwell, G. *1984*. (Trad. Rafael Vázquez Zamora). Editorial Austral, Ediciones Destino. Madrid, 2010.

Palazzi, P. *La Protección de los Datos Personales en Argentina*. Ed. Errepar. Buenos Aires, 2004.

Pérez Luño, A. *Derechos Humanos, Estado de Derecho y Constitución*. Editorial Tecnos, 5ª Edición. Madrid, 1995.

Peyrano, G. *Régimen legal de los datos personales y habeas data*. Editorial LexisNexis – Depalma. Buenos Aires, 2001.

Pierini, A.; Lorences V.; Tornabene, M. *Habeas Data. Derecho a la Intimidad*. Editorial Universidad. Buenos Aires, 1998.

Ponzetti de Balbín, Indalia c/ Editorial Atlántida S.A. C.S., 1984/12/11. Editorial La Ley. Suplemento Universitario La Ley. Buenos Aires, 2001.

Puccinelli, O. *El Habeas Data en Indoiberoamérica*. Editorial Temis. Bogotá, 1999.

Quiroga Lavié, H. *Habeas Data.*Editorial Zavalía, Buenos Aires, 2001.

Rebollo Delgado, L. *Derecho Fundamentales y Protección de Datos*. Editorial Dykinson. Madrid, 2004.

Rebollo Delgado, L. *El derecho fundamental a la intimidad*. Editorial Dykinson (2ª Edición Actualizada). Madrid, 2005.

Rebollo Delgado, L. y Serrano Pérez, M. *Introducción a la Protección de los datos*. 2ª Ed. Editorial Dykinson. Madrid, 2008.

Revista Privacy Law & Business & Newsletter; Edición de Agosto de 1997.

Rodríguez, A. W.; Galeta de Rodríguez, B. *Diccionario de Latín Jurídico. Locuciones latinas y su aplicación jurídica actual*. Editorial García Alonso. Buenos Aires, 2006.

Rodríguez Domínguez, E. *Derecho Procesal Constitucional*. 2ª ed. Editorial Jurídica GRIJLEY E.I.R.L. Lima, (Perú), 1999.

Romero, J. L. *Breve historia de la Argentina*. Editorial Fondo de Cultura Económica de Argentina. Buenos Aires, 1996.

Romero, J. L. *Breve historia de la Argentina*. 3ª reimpresión. Editorial Fondo de Cultura Económica de Argentina. (Colección Tierra Firme). Buenos Aires, 1999.

Sagués, N. "El nuevo Código Procesal Constitucional de la Provincia de Tucumán". Publicado en la Revista de Derecho Procesal: *Amparo, habeas data, habeas corpus – I*. Editorial Rubinzal-Culzoni Editores; Santa Fe (Argentina), 2000.

Saltor J. *La ciencia y el mundo de la vida*. Editorial UNSTA. Tucumán, 2011.

Santamaría Ramos, F. *El encargado independiente. Figura clave para un nuevo derecho de protección de datos*. Editorial la Ley. Madrid, 2011.

Sbdar, C. (Directora y Coordinadora). *Estudio del Amparo en la Nación y en la Provincia de Tucumán. Competencia – Admisibilidad – Trámite – Recursos – Cosa Juzgada*. Editorial ER Ediciones del Rectorado. Universidad Nacional de Tucumán, 2006.

Suñé Llinás, E. "La protección de la intimidad en el sector de las telecomunicaciones". Comunicación publicada en las Actas del XII encuentro sobre Informática y Derecho 98/99, (obra coordinada por Miguel Ángel Davara Rodríguez). Editorial Aranzadi. Pamplona, 1999.

Suñé Llinás, E. *Tratado de Derecho Informático. Volumen I: Introducción y Protección de Datos Personales*. Segunda Edición (Actualizada por Cristina Almuzara Almaida). Editorial Servicio de Publicaciones Facultad de Derecho de la Universidad Complutense de Madrid. Madrid, 2002.

Suñé Llinás, E. y Santamaría Ramos, F. *Comentarios al art. 43*. Responsables y Encargados del Tratamiento, p. 2017. Publicado en: Troncoso Reigada A. (Director). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Editorial Civitas y Thomson Reuters (Editorial Aranzadi). Pamplona (España), 2010.

Terceiro, J. *Sociedad Digital. Del homo sapiens al homo digital*. Editorial Alianza. Madrid, 1996.

Toffler, A. *El Cambio del Poder*. (Trad. Rafael Aparicio). Plaza y Janes Editores S. A. (4ª edición). Madrid, 1995. Titulo original de la obra: *Power Shift*.

Toynbee, A. *Estudios de la Historia*. Compendio IX/XIII (Tomo 3). Sexta reimpresión. Editorial Alianza. Madrid, 1991.

Warren, S.; Brandeis, L. *El derecho a la intimidad*. (Trad. del inglés de Pendas, B. y Baselga, P.). Editorial Civitas. Madrid, 1995.

Warren, S.; Brandeis, L. "The Right to Privacy". Revista de la Universidad de Harvard: 4 Harvard Law. Rev. Cambridge, Massachusetts (EEUU), 1890.

White Paper: Computers and Privacy. Editorial HMSO, Londres (GB), 1975.

Uicich, R. *Habeas Data. Ley 25.326*.Ed.*Had Doc*. Buenos Aires, 2001.

Urabayen, M. *Vida Privada e Información. Un conflicto permanente*. EUNSA (Ediciones de la Universidad de Navarra S.A.). Zaragoza (España), 1977.

Zapater Carón, J. *La libertad en Karl Jasper*. Editorial Librería General. Zaragoza, 1981.

Zavala de González M. *Derecho a la Intimidad*. Editorial Abeledo-Perrot. Buenos Aires, 1982.

WEBGRAFÍA

Por orden de Alfabético:

Acuerdo de Schengen: http://publicaronline.net/2010/04/05/acuerdo-schengen-nuevas-disposiciones-de-visado-para-la-union-europea/

Agencia Española de Protección de Datos (España): https://www.agpd.es

Alto Comisionado de Privacidad (Autoridad de control en materia de protección de datos personales de Canadá): http://www.priv.gc.ca/index_e.asp

Asamblea Legislativa de la República de Costa Rica:
www.racsa.co.cr/asamblea

Audiencia pública realizada en la ciudad de San Miguel de Tucumán el 5/9/2012 sobre la reforma del Código Civil argentino. En este sitio pueden consultarse las ponencias, los videos y las versiones taquigráficas de las comunicaciones presentadas ante la Comisión Bicameral de Reforma del Código Civil: http://ccycn.congreso.gov.ar/convocatoria/06-09.html

B.V.K (sigla que responde a su nombre en neerlandés: Beroepsvereniging van het Krediet, en castellano Unión Profesional de Crédito, Bélgica):
http://www.upc-bvk.be/

Boletín Oficial del Estado (España): http://www.boe.es/

Caso Urteaga, Facundo Raúl c/ Estado Mayor Conjunto de las Fuerzas Armadas s/ amparo - ley 16.986 (Argentina: Jurisprudencia):
http://www.planetaius.com.ar/fallos/jurisprudencia-u/caso-Urteaga-Facundo-Raul-c-Estado-Nacional-Estado-Mayor-Conjunto-de-las-FF-AA.htm

COBAC (entidad de crédito de Bélgica):
http://assecuranz.kompass.com/en/Belgium/Euler-Cobac%20Belgium%20SA-NV/BE504431-dir.php

Código Civil (Argentina).

College Bescherming Persoonsgegevens (CBP – autoridad de control holandesa en material de protección de datos): http://www.cbpweb.nl

Constitución de la República Federativa de Brasil (reformada en 1988):
http://www.georgetown.edu/pdba/Constitutions/Brazil/brazil88.html

Concejo de Europa: http://www.coe.int/

Congreso de Colombia (Senado): http://www.senado.gov.co/Senado/senadoa.htm

Constitución Española (Diciembre de 1978):
http://www.congreso.es/funciones/constitucion/indice.htm

Constitución del Estado Plurinacional de Bolivia (2009):
http://bolivia.infoleyes.com/shownorm.php?id=469

Constitución Europea:
http://www.unizar.es/centros/fderez/doc/ConstitucionEuropea.pdf

Constitución Política del Perú (1993):
http://www.georgetown.edu/pdba/Constitutions/Peru/peru.html

Constitución de la República Bolivariana de Venezuela (2000):
http://www.cgr.gob.ve/contenido.php?Cod=048

Convenio 108 para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (Consejo de Europa), 1985: http://www.ifai.org.mx/pdf/ciudadanos/sitios_de_interes/datos_personales/Convenio108.pdf
También en: http://www.judicatura.com/Legislacion/1999.pdf

Comisión de Protección de Datos de Austria: https://www.dsk.gv.at/

Commission Nationale de L`Informatique et des Libertés (Francia): http://www.cnil.fr/

Comisionado de Protección de Datos (*Data Protection Commissioner* – Irlanda): http://www.dataprivacy.ie/

Comisionado para la Protección de Datos (Autoridad de control en materia de protección de datos - Reino Unido de Gran Bretaña). Fci.: http://www.ico.gov.uk/

Comisión Nacional de Protección de Datos (CNPD – autoridad de control en materia de protección de datos personales de Portugal): http://www.cnpd.pt/
Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica): http://www.cajpe.org.pe/RIJ/bases/instru/ib1.HTM

Constitución de la República Argentina con sus reformas de 1994. : http://www.senado.gov.ar/web/constitucion/cuerpo1.html

Constitución Política de la República de Chile (1989):
http://www.georgetown.edu/pdba/Constitutions/Chile/chile89.html

Constitución Política de la República de Costa Rica (1996):
http://www.constitution.org/cons/costaric.htm

Constitución Política de la República de Colombia: www.senado.gov.co
http://pdba.georgetown.edu/constitutions/colombia/col91.html

Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica): http://www.oas.org/juridico/spanish/firmas/b-32.html

Corte Suprema de Justicia de la Nación Argentina. www.pjn.gov.ar

Cour des Comptes (Tribunal de Cuentas francés): http://www.ccomptes.fr/

Corte Constitucional de la República de Colombia:
http://www.corteconstitucional.gov.co/

Corte Suprema de Justicia de Costa Rica: Sala Constitucional:
http://www.poder-judicial.go.cr/salaconstitucional/

Corte Suprema de Justicia de El Salvador: http://www.csj.gob.sv/

Data Surveillance Authority (autoridad de control danesa) en castellano Agencia de Protección de Datos Personales de Dinamarca: http://www.datatilsynet.dk/eng/

Dirección Nacional de Protección de datos Personales (autoridad de control de protección de datos personales, Argentina):
http://www.jus.gob.ar/datos-personales.aspx

Directrices para la armonización de la Protección de Datos en la Comunidad Iberoamericana, Bolivia (2006). Grupo de Trabajo Permanente de Desarrollo Normativo de la Red Iberoamericana de Protección de Datos.
http://www.redipd.org/reuniones/encuentros/V/common/9_nov/Directrices_de_armonizacion.pdf

Constitución Política de la República de Ecuador (1998):
http://www.georgetown.edu/pdba/Constitutions/Ecuador/ecuador98.html

Constitución de la República de El Salvador:
http://www.constitution.org/cons/elsalvad.htm

Directiva 97/46/CE:
http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/ common/pdfs/B.5-cp--Directiva-97-66-CE-.pdf

Directiva 2002/58/CE de 12 de julio de 2002 (Unión Europea): http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:es:HTML

Diccionario de la Lengua Española, Vigésima Segunda Edición:
http://lema.rae.es/drae/

Dirección Nacional de Protección de Datos Personales (Argentina): www.jus.gov.ar/dnpdp

Diario oficial (Bélgica): http://www.moniteur.be/

Fallo Halabi, Ernesto c/ P.E.N. – Ley 25.873 – Decreto N° 1563/04 s/amparo Ley 16.986. (Inconstitucionalidad y tráfico de datos - Argentina):
http://www.hfernandezdelpech.com.ar/JurisprudenciaArgFalloHalabi.html
Este fallo también puede consultarse en:
http://www.iprofesional.com/notas/78867-Fallo-Halabi-Ernesto-c-PEN---ley-25873---dto-156304-s-amparo-ley-16986.html

Fernández Delpech. A. *Protección de Datos Personales – Derecho al olvido* Universidad del Salvador, 2008:
http://www.hfernandezdelpech.com.ar/Trabajo%20Derecho%20al%20Olvido.pdf

Garante de la Protección de Datos Personales (Garante per la Protezione dei Dati Personali – Autoridad de Control - Italia):
http://www.garanteprivacy.it

Instituto Federal de Acceso a la Información y Protección de Datos:
http://www.ifai.org.mx/

Grupo de Trabajo Sobre Protección de Datos de la Unión Europea. Dictamen 4/2002 sobre el nivel de protección de datos en la República Argentina, (sobre el art. 29) Informe 11081/02/ES/ Final – WP 63 del 3 de Octubre de 2002, p. 14.: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp63_es.pdf

Junta de Inspección de Datos (*Datainspektionen* – autoridad de control en materia de protección de datos - Suecia): http://www.datainspektionen.se

Junta de Protección de Datos (Noruega): http://www.datatilsynet.no/

La Gaceta, (diario de la Provincia de Tucumán, Argentina). "Venden todo lo que la web sabe de nosotros", edición en papel del día 25 de Agosto de 2012: http://lagaceta.com.ar/nota/507515/economia/red-no-gratis-vos-pagas-tus-datos.html

Ley 21.173 (Argentina), 1975. Ley sobre el derecho a la intimidad en el Código Civil argentino: http://federacionuniversitaria21.blogspot.com/2008/08/ley-21173-derecho-la-intimidad.html

Ley Nº 9.507 (Brasil), 1997. Esta ley desarrolla el instituto del habeas data, regulando el derecho al acceso a informaciones y su trámite procesal en Brasil: http://www.dhnet.org.br/direitos/brasil/leisbr/acesso/habeasdata/

Ley de Protección de la Información Personal y de los documentos electrónicos (Canadá), 2000. Esta ley es conocida como la ley PIPEDA, Bill C-6, fue reformada en 2011: www.justice.gc.ca

Ley Federal de Protección de Datos Personales en Posesión de Particulares (México): http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Fundamental de la República Federal Alemana (Bonn, 1949). Más conocida con Ley Fundamental de Bonn.
Fci.:http://www.buenos-aires.diplo.de/contentblob/2227504/Daten/375140/Grundgesetz_Download.pdf

Ley 26301 sobre la aplicación de la acción constitucional de habeas data (Perú), 1994:
http://www.bomberojuridico.com.ar/pagproductos/version_limitada/habeas_data/habeas_data_nuevo/legislacion/hd_ley_peru.htm

Ley de Protección de Datos Personales Nº 67/98, de 26 de octubre (Portugal): http://www.cnpd.pt/bin/legis/leis_nacional.htm

Ley de Protección de Datos Personales, BDSG – 1990, (Alemania):
http://www.gesetze-im-internet.de/bdsg_1990/

Ley de Protección de Datos Personales, *Datenschutzgesetz* (DSG) -1978- (Austria):
www.kronegger.at

Ley de Protección de Datos Personales (Bélgica) del 8 de diciembre de 1992. Ver en el sitio web de la Comisión para la Protección de la Vida Privada (autoridad de control en materia de protección de datos personales del Reino de Bélgica):
www.privacy.fgov.be

Ley de Protección de Datos de (Dinamarca), Nº 429, del 31 de mayo de 2000: http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/

Ley Orgánica de Regulación del Tratamiento Automatizado de Datos Personales N° 5/1992 (LORTAD - España): http://sdi.uc3m.es/seguridad/lortad.html

Ley Orgánica de Protección de Datos (LOPD - España) Nº 15/1999: https://www.agpd.es/index.php

Ley Orgánica 1/82 (España): http://www.boe.es/aeboe/consultas/bases_datos/doc.php?coleccion=iberlex&id=1982/11196

Ley N° 78-17 del 6 de enero de 1978, relativa a la informática, a los ficheros y a las libertades (Francia), con la modificación del año 2004: http://www.cnil.fr/fileadmin/documents/es/Lei78-17VE.pdf

Ley número 2472 de 1997 de protección de las personas con respecto al tratamiento de los datos de carácter personal (Grecia), junto con sus modificatorias en Ingles. Puede ser consultada en el sitio web de la *Hellenic Data Protection Authority* (autoridad de control griega): http://www.dpa.gr/legal_eng.htm

Ley 25.892 de Protección de Datos Personales de 23 de noviembre de 1999 (*Wetbescherming Persoonsgegevens* - Holanda)[615]:http://www.cbpweb.nl
También puede ser consultada en: http://home.planet.nl/~privacy1/wbp.htm

Ley de protección de datos personales del 13 de julio de 1988 (Irlanda): http://www.dataprivacy.ie/6ai.htm

Ley de Protección de Datos Personales Nº 675/96 de 31 de diciembre de 1996 (Italia). Texto consolidado el 28 de diciembre de 2001: http://www.garanteprivacy.it/garante/frontdoor/1,1003,,00.html?LANG=1

Ley para la regulación de las Sociedades de Información Crediticia (México), 2002: http://www.shcp.gob.mx/servs/normativ/leyes/l_rsic.html

Ley sobre el Tratamiento de Datos Personales Nº 2000-04-14-31 (Noruega), 2000: http://translate.googleusercontent.com/translate_c?hl=es&prev=/search%3Fq%3Dhttp://www.datatilsynet.no/%26hl%3Des%26rlz%3D1G1TSLA_ESAR439%26prmd%3Divns&rurl=translate.google.com.ar&sl=no&u=http://www.lovdata.no/all/nl-20000414-031.html&usg=ALkJrhjyJa6OcSG3JXJwaBLo7NHXoOLQ-Q

[615] En este sitio web se puede encontrar la ley holandesa de protección de datos personales en su idioma original y en inglés.

Ley N° 17.838 (Uruguay), 2004. Ley de Protección de Datos Personales para ser Utilizados en Informes Comerciales y Habeas Data: http://200.40.229.134/leyes/AccesoTextoLey.asp?Ley=17838&Anchor

Freedom of InformationAct (Ley de Libertad de la Información - EEUU), FOIA: http://www.usdoj.gov/04foia/1974compmatch.htm

Privacy Act (Ley de Protección de la Intimidad - EEUU), 1974: http://www.usdoj.gov/04foia/1974compmatch.htm

Fair Credit ReportingAct (Ley de Equidad Financiera - EEUU), 1978. Esta ley fue modificada en diferentes momentos. http://www.ftc.gov/os/statutes/fcradoc.pdf

MERCOSUR: www.mercosur.org.uy/

Monitor de Privacidad y Acceso a la Información en América Latina: http://www.privacidadyacceso.org/

Organización para la Cooperación y el Desarrollo Económico: http://www.oecd.org

Organismo de Reguladores Europeos de Comunicaciones Electrónicas (ORECE): http://sociedaddelainformacion.wordpress.com/2010/01/28/el-orece-nuevo-regulador-de-las-telecomunicaciones-de-la-union-europea-inicia-su-actividad/

Proyecto de Ley estatutaria Nº 184 de 2010 del Senado de Colombia y 046 de 2010 de la Cámara de Diputados (Colombia): http://www.senado.gov.co/Senado/senadoa.htm

Proyecto de Código Civil y Comercial de la Nación (Argentina), 2011: www.nuevocodigocivil.com

Comisionado Federal para la Protección de Datos y Libertad de Información (Autoridad de Control, Alemania): www.datenschutz.bund.de

Sentencia del Tribunal Constitucional Alemán relativa a Ley del Censo (1983): http://www.informatica-juridica.com/jurisprudencia/alemania.asp

Sentencia del Tribunal Constitucional Español (TCE, España), Sala Civil, 4 de Noviembre de 1986. http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=1167504&links=la%20delimitacion%20de%20la%20esfera%20de%20la%20intimidad&optimize=20051011

Sentencia del Tribunal Constitucional Español (TCE, España) por la que se declara la inconstitucionalidad de algunos artículos de la ley LOPD, al resolver en el año 2000 un recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. Recurso Nº1563-2000, cuya sentencia fue publicada en el Boletín Oficial del Estado de fecha 4/01/2001: http://www.boe.es/

Tratado de Asunción. Tratado constitutivo del MERCOSUR (Argentina, Brasil, Paraguay y Uruguay), 1991: http://www.mercosur.int/innovaportal/file/655/1/CMC_1991_TRATADO_ES_Asuncion.pdf

Tribunal Constitucional Alemán: http://www.bundesverfassungsgericht.de/

Tratado de Roma (Unión Europea): http://es.wikisource.org/wiki/Constituci%C3%B3n_de_la_Uni%C3%B3n_Europea

Warren, S.; Brandeis, L. "The Right to Privacy". Vol. 4, N° 5, Harvard Law Rev (Revista Jurídica de la Universidad de Harvard). Cambridge, Massachusetts (EEUU), 1890: http://www.law.louisville.edu/library/collections/brandeis/node/225

LEGISLACIÓN CONSULTADA

Acuerdo de Schengen.

Tratado de Roma[616].

Código Penal (Uruguay).

Código Penal (Argentina). Artículos 117 bis y 157 bis.

Convenio 108 del Consejo de Europa para la protección de las personas con relación al tratamiento de los datos de carácter personal.

Constitución Argentina (1994).

Constitución de la República Federativa de Brasil (1988).

Constitución de la República Bolivariana de Venezuela (2000).

Constitución Política de Colombia (1991). Reformada en 2005.

Constitución de España (1978).

Constitución del Estado Plurinacional de Bolivia (2009).

Constitución Política de la República de Chile (1991)

Constitución Política de la República de Costa Rica.

Constitución de la República de Ecuador (1998).

Constitución de la República Helénica (2001).

Constitución de la República de Nicaragua.

Constitución de la República de Panamá (2004).

Constitución de la República de Paraguay (1992).

Constitución Política del Perú (1993).

Constitución de Portugal (1976).

[616] El Tratado de Roma es el instrumento jurídico que aprueba la Constitución Europea. El día 29 de octubre de 2004 se procedió a la firma del mismo en la ciudad de Roma.

Constitución de la República de El Salvador.

Constitución de la República Oriental del Uruguay.

Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica).

Código Procesal Penal (Colombia).

Decreto-Ley Nº 15.322 (Uruguay).Regula el Sistema de Intermediación Financiera.

Decreto N° 1616/96 del P.E.N. (Argentina), 1996. Por medio de este Decreto el PEN argentino vetó totalmente a la primera ley N° 24.745 de Protección de Datos Personales.

Decreto Nacional 1558/2001 (Argentina), 2001. Reglamenta el artículo 29 de la ley 25.326,a partir del cual se crea la Dirección Nacional de Protección de Datos Personales

Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995 (Unión Europea), relativa a la protección de las personas físicas en lo referido al tratamiento de los datos personales y a su libre circulación.

Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Luego derogada por la Directiva 2002/58/CE.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo de Europa de 12 de julio de 2002 (Unión Europea), relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas.

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones (también modifica la directiva 2002/58/CE).

Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 (modifica la directiva 2002/58/CE). Modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas,

Reglamento (CE) Nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.

Ley sobre Acceso a la Información Pública N° 621 (Nicaragua), 2007.

Ley Nº 7135 de la Jurisdicción Constitucional (Costa Rica), 1989.

Ley 26301 sobre la aplicación de la acción constitucional de habeas data (Perú), 1994.

Ley 19.628 sobre Protección de la Vida Privada (Chile), 1999. Modificada por la ley 19.812 del año 2002.

Ley de Protección de Datos del Estado de Hesse (Alemania) de 7 de Octubre de 1970.

Ley 16.986 por la cual se reglamentan los amparos (Argentina).

Ley N° 24.745 (Argentina), 1996. Esta primera ley de Protección de Datos fue vetada totalmente por el PEN.

Ley 26.388 (Argentina), 2008. Modificó el Código Penal.

Ley Federal para la protección contra el uso ilícito de Datos Personales - (Alemania), 1977. Sustituida por la vigente Ley de Protección de Datos (conocida como BDSG), promulgada el 20 diciembre de 1990.

Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010.
Ley de Protección de Datos Personales (Austria). Conocida en alemán con el nombre de Datenschutzgesetz (DSG, 1978), el 18 de octubre de 1978. Modificada por la Ley Federal de Protección de Datos de Carácter Personal (Bundesgesetzüber den Schutz Personenbezogener Daten / Datenschutzgesetz 2000 - DSG 2000), 2000.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (México), 2002.

Ley Fundamental de la República Federal Alemana (Bonn, 1949). Más conocida con Ley Fundamental de Bonn.

Ley Federal de Protección de Protección de Datos Personales en Posesión de los particulares (México), 2010.

Ley Nacional de Protección de Datos Personales (Argentina): Ley Nº 25.326.

Ley de Protección de Datos Personales (Bélgica) del 8 de diciembre de 1992.

Ley de Protección de la Información Personal y de los documentos electrónicos (Canadá), 2000. Esta ley es conocida como la ley PIPEDA, Bill C-6, fue reformada en 2011.

Ley 221/2007 (Colombia), por la cual se desarrolla al artículo 15 de la Constitución Política de Colombia y se establece una regulación legal infra constitucional a la protección de los datos de carácter personal.

Ley de Privacidad (EEUU) del 31 de diciembre de 1974.

Ley 10/91 de Protección de Datos Personales frente a la Informática. Posteriormente esta ley fue reemplazada por la Ley de Protección de Datos Personales Nº 67/98, de 26 de octubre de 1998 (Portugal).

Ley de Protección de Datos Personales Nº 429, del 31 de mayo de 2000 (Dinamarca).

Ley Orgánica de Protección de Datos (LOPD - España): L.O. 15/99.

Ley sobre Protección de la Vida Privada (Chile) Nº 19628.

Ley N° 78-17 del 6 de enero de 1978, relativa a la informática, a los ficheros y a las libertades (Francia).

Ley de Protección de Datos Personales (Data ProtectionAct – Gran Bretaña), 1984.

Ley de Protección de Datos (DataProtectionAct – Gran Bretaña), 1998. Entró en vigencia en el Reino Unido de Gran Bretaña el 1 de marzo de 2000, revocando la Ley de Protección de Datos de 1984

Ley de Libertad de Información (Freedom of Information Act – Gran Bretaña), 2000.

Ley 6/2002 Nº 24.476 sobre Protección de Datos (Panamá), 2002.

Ley de Libertad de la Información (Freedom of Information Act, FOIA -EEUU).

Ley Orgánica de Regulación del Tratamiento Automatizado de Datos Personales N° 5/1992 (LORTAD - España).

Ley N° 2472 de 1997 de Protección de las Personas con Respecto al Tratamiento de los Datos de Carácter Personal (Grecia).

Ley 25.892 de Protección de Datos Personales de 23 de noviembre de 1999 (*Wetbescherming Persoonsgegevens* – Holanda).

Ley de Protección de Datos Personales Nº 675/96 del 31 de diciembre de 1996 (Italia). Texto consolidado el 28 de diciembre de 2001.

Ley de Datos (*The Data Act- Suecia*) N° 1973/289, vigente a partir del 1 de julio de 1973. Modificada primero en 1989 y luego remplazada en 1998 por la ley de Protección de Datos (*The Personal Data Act* - Suecia) Nº 1998/204, que comenzó a regir plenamente a partir del 30 de septiembre de 2001.

Ley de Información de Crédito N° 1973/1173 (The Credit Information Act – Suecia), 1973. Esta ley regula la recolección y el tratamiento de datos personales de crédito.

Ley de Control Constitucional (Ecuador), 1997.

Ley de Recuperación de Deudas (*The Debit Recovery Act* - Suecia), 1974.

Ley sobre el Tratamiento de Datos Personales Nº2000-04-14-31 (Noruega), 2000.

Ley Nº 9.507 de Habeas Data (Brasil), 1997.

Ley 26.301 de Habeas Data (Perú), 1994.

Ley 27.489 (Perú), 2001.

Ley 21.173 (Argentina), 1975. Ley sobre el derecho a la intimidad en el Código Civil argentino.

Ley de Entidades Financieras Nº 21.526 (Argentina).

Ley 1682 (Paraguay), 2000. Esta ley desarrolló la norma constitucional yreglamentó el uso de la información de carácter privado.

Ley para Regular las Sociedades de Información Crediticia (México), 2002.

Ley N° 14.306 (Uruguay). Código Tributario de Uruguay.

Ley N° 16.011 (Uruguay). Esta ley reglamenta el recurso de amparo en Uruguay.

Ley Nº 16.099 (Uruguay). Esta ley se ocupa de la libertad de comunicación, de pensamiento e información.

Ley N° 16.016 (Uruguay). Esta ley regula el Sistema Estadístico de Uruguay, sobre los deberes de pertinencia, transparencia, confidencialidad y finalidad.

Ley N° 17.838 (Uruguay), 2004. Ley de Protección de Datos Personales para ser Utilizados en Informes Comerciales y Habeas Data.

Ley de Reforma Parcial de la Ley del Banco Central de la República Bolivariana de Venezuela (Venezuela), 2009.

Proyecto de Ley estatutaria Nº 184 de 2010 del Senado de Colombia y 046 de 2010 de la Cámara de Diputados (Colombia).

Proyecto de Unificación de la legislación civil y comercial (Argentina), 1987.

Proyecto de Código Civil y Comercial de la Nación (Argentina), 2011.

Real Decreto 1736/1998 (España).

Tratado de Roma.

Tratado de Asunción. Tratado constitutivo del MERCOSUR (Argentina, Brasil, Paraguay y Uruguay), 1991.

INFORMACIÓN ADMINISTRATIVA

Universidad Complutense.

Facultad de Derecho.

Departamento de Filosofía, Moral y Política I

Programa 1510096001 – Conceptos Jurídicos Fundamentales

Tesis Nº 99952942

INDICE DE CAPÍTULOS

ABREVIATURAS	7
RESUMEN EN INGLÉS	11
CAPÍTULO I: JUSTIFICACIÓN	17
CAPÍTULO II: PROTECCIÓN DE LOS DATOS EN ESPAÑA Y EUROPA	155
CAPÍTULO III: PROTECCIÓN DE LOS DATOS EN AMÉRICA	272
CAPÍTULO IV: PROTECCIÓN DE LOS DATOS EN ARGENTINA	366
CAPÍTULO V: CONCLUSIONES	465
RECURSOS BIBLIOGRÁFICOS	487
BIBLIOGRAFÍA	487
WEBGRAFÍA	492
LEGISLACIÓN CONSULTADA	502
INFORMACIÓN ADMINISTRATIVA	508

Contenido

ABREVIATURAS 8

RESUMEN EN INGLÉS 11

Introduction 11
Objective: Research Content 12
Conclusions / Results 14
Bibliography 15

Capítulo I: JUSTIFICACIÓN 17

1.- Cuestiones metodológicas 17
1.1.- Hipótesis 20
1.2.- Punto de Partida 20
1.3.- Antecedentes 22
2.- Intimidad y procesamiento de datos 23
2.1.- Sobre el concepto de derecho a la intimidad 28
2.2.- Diferencias con otras manifestaciones de la personalidad 39
2.2.1. Lo confidencial 39
2.2.2. Lo secreto 40
2.2.3. Lo íntimo 40
2.2.4.- Honor y propia imagen 44
2.2.5.- Usos sociales y conducta del sujeto 48
2.2.6.- Derecho al olvido 51
2.3.- Intimidad y autodeterminación informativa 56
2.4.- Intimidad y protección de los datos 65
2.5.- Evolución histórica de la idea de intimidad 73
2.5.1.- Edad Antigua 74
2.5.2.- Edad Media 78
2.5.3.- Edad Moderna 82
2.5.4.- Edad Contemporánea 85
2.5.5.- Siglos XX y XXI 87
2.6.- La intimidad de las personas jurídicas 96
3.- Reconocimiento Internacional 98
3.1.- Recomendación de la OCDE 107
4.- Técnicas legislativas aplicadas a la protección de datos 109
4.1.-Leyes Sectoriales 109
4.2.- Leyes Ómnibus 110
5.- Habeas Data 111
6.- Jurisprudencia del Tribunal Constitucional español sobre protección de datos 114
6.1.- Sentencia 290/2000 de 30 de noviembre 115
6.2.- Sentencia 254/1993 de 20 de julio 116
6.3.- Sentencia 292 de 30 de noviembre de 2000 123
6.3.1.- Importancia de la STC 292/2000 127
6.3.2.- ¿Protección de datos o autodeterminación informativa en la STC 292/2000? 132
7.- Principios de la protección de los datos de carácter personal 135
8.- Autoridad de control para la protección de los datos 140
8.1.- Autoridad de control independiente 142
8.2.- Autoridad de control dependiente del Poder Ejecutivo 146
8.3.- Sistema de control judicial de aplicación de la ley 148
8.4.- El encargado de protección los datos 149
9.- Datos personales y telecomunicaciones 150

CAPÍTULO II: PROTECCIÓN DE DATOS EN ESPAÑA Y EUROPA 155

1.- El Consejo de Europa 155
1.1.- Las Resoluciones (73) 22 y (74) 29 del Comité de Ministros 155
1.2.- El Convenio 108 del Consejo de Europa 156
2.- Antecedentes en el derecho europeo 163
2.1.- Acuerdo de Schengen de 14 de junio de 1985 166
2.2.- Directiva 95/46/CE 169
2.3.- Directiva 58/2002/CE del Parlamento Europeo y del Consejo 174
2.4.- Directiva 97/66/ CE 177
2.5.- Nuevas normas europeas 179
2.6.- Proyecto de la Comisión Europea del año 2012 180
2.6.1.- Control ciudadano 183
2.6.2.- Protección de datos en el mercado digital 184
2.6.3.- Globalización y protección de los datos 186
2.7.- La protección de datos en la Constitución Europea 187
3.- España 190
4.- Alemania 201
5.- Austria 209
6.- Bélgica 215
7.- Dinamarca 222
8.- Francia 226
9.- Grecia 237
10.- Holanda 243
11.- Irlanda 246
12.- Italia 250
13.- Portugal 252
14.- Reino Unido 256
15.- Suecia 263
16.- Noruega 268

CAPÍTULO III: PROTECCIÓN DE DATOS EN AMÉRICA 272

1.- Estados Unidos de América. 274
1.1.- Autoridad de aplicación en EEUU 281
1.2.- Bancos de Datos de Información de Crédito 281
1.3.- Seguridad 284
2.- Bolivia 284
3.- Brasil 287
4.- Perú 294
5.- Nicaragua 301
6.- Panamá 304
7.- Canadá 309
8.- Colombia 313
9.- Chile 320
10.- Costa Rica 324
11.- Ecuador 333
12.- México 339
13.-Paraguay 345
14.- Uruguay 347
15.- Venezuela 354
16.- El Salvador 358
17.- MERCOSUR 360
18.- Cuadro comparativo de algunas normas americanas 365

CAPÍTULO IV: PROTECCIÓN DE DATOS EN ARGENTINA 366

1.- Un nuevo derecho en Argentina 366
2.- Intimidad y datos personales en la historia argentina 367
3.- Reforma constitucional de 1994 375
3.1.- Doctrina y jurisprudencia 377
3.2.- *Habeas Data*: naturaleza jurídica y trámite procesal 378

3.2.1.- Legitimación activa en la acción de *habeas data* 381
3.2.2.- Legitimación pasiva en la acción de *habeas data* 384
4.- Desarrollo normativo del artículo 43 ter. 384
4.1.- La vetada ley sobre *habeas data* N° 24.745 384
4.2.- Decreto Nacional 1616/96 385
4.3.- Proceso de formación de la Ley 25.326 392
4.4.- Decreto Nacional 1558/2001 393
5.- Ley 25.326 de Protección de Datos Personales 396
5.1.- Objeto de la ley 25.326 400
5.2.- Datos personales y otros conceptos 401
5.3.- Principios de protección de datos 403
5.3.1.- Licitud de la formación de archivos de datos 403
5.3.2.- Prohibición de acumulación de datos sensibles 403
5.3.3.- Prohibición de bancos de datos que no reúnan condiciones de seguridad 404
5.3.4.- Principio de confidencialidad 404
5.3.5.- Principio de Buena Fe 406
5.4.- Cesión de Datos Personales 407
5.5.- Obligaciones del cesionario 407
5.6.- Transferencia internacional de datos 409
5.7.- Derechos de los titulares de los datos 410
5.7.1.- Derecho a la información 410
5.7.2.- Derecho de acceso 411
5.7.3.- Derecho a conocer el contenido de la información 411
5.7.4.- Derecho de rectificación de datos personales 412
5.7.5.- Derecho de actualización de los datos personales 412
5.7.6.- Derecho de supresión de los datos personales 413
5.7.7.- Derecho a impugnar valoraciones personales 413
5.7.8.- Gratuidad en el ejercicio de los derechos del titular 413
5.7.9.- Excepciones 413
6.- Comisiones legislativas 414
7.- Usuarios y responsables de archivos, registros y bancos de datos 415
8.- Archivos, registros o bancos de datos privados 417
9.- Prestación de servicios de información crediticia 418
10.- Archivos, registros o bancos de datos con fines de publicidad 420
11.- Archivos, registros o bancos de datos relativos a encuestas 420
12.- Órgano de control 420
13.- Códigos de conducta 423
14.- Sanciones administrativas y penales 425
15.- Etapas del proceso de protección de datos personales 427
15.1.- Etapa extrajudicial 427
15.2.- Etapa judicial de protección de datos personales 428
16.- Jurisprudencia 437
16.1.- Jurisprudencia anterior a la reforma constitucional de 1994 437
16.2.- Jurisprudencia posterior a la reforma constitucional de 1994 438
17.- Antecedentes en el derecho público provincial argentino 443
17.1.- Protección de datos en la Provincia de Tucumán (Argentina) 456
CAPÍTULO V: CONCLUSIONES 465

1.- Problema 465
1.1.- Tecnología y procesamiento de datos 465
1.2.- Uso masivo de las TIC 466
1.3.- Efectos de la conducta de las personas en el mundo virtual 467
1.4.- Las Redes Sociales 469
2.- Recolección de Datos 470
2.1.- Utilidad del método comparativo 470
2.2.- Legislación de protección de datos personales 471
2.3.- La jurisprudencia 473
2.4.- Legislación Europea 474
2.5.- Legislación americana 474

2.6.- La protección de datos personales en Argentina 476
3.- Resultados 480
Primera conclusión 480
Segunda conclusión 480
Tercera conclusión: propuestas para mejorar la legislación Argentina 484
Reflexión final 486
RECURSOS BIBLIOGRÁFICOS 487
BIBLIOGRAFÍA 487
WEBGRAFÍA 494
LEGISLACIÓN CONSULTADA 502
INFORMACIÓN ADMINISTRATIVA 508
INDICE DE CAPÍTULOS 509